LAUREA PUBLICATIONS
B•37

LAUREA

Rauno Pirinen, Jyri Rajamäki (ed.)

INTEGRATIVE STUDENT-CENTERED RESEARCH AND DEVELOPMENT WORK

Sample of Evidence Series: Volume (1)

Rescuing of Intelligence and Electronic Security Core Applications (RIESCA)

Edited May 2010

Laurea publications
B•37

INTEGRATIVE STUDENT-CENTRED RESEARCH AND DEVELOPMENT WORK

Sample of Evidence Series: Volume (1)

Rescuing of Intelligence and Electronic Security Core Applications (RIESCA)

Rauno Pirinen, Jyri Rajamäki (ed.)

Edited May 2010

2010 Espoo

Picture of cover page is from lake Iijärvi, Paltamo, Kainuu, Finland
by Merja and Jyri 2009

ISSN 1458-7238
ISBN 978-951-799-206-0

Edita Prima Oy, Helsinki 2010

Table of Contents

FOREWORD 5

PART I - Introduction 7

RIESCA, RESCUING OF INTELLIGENCE AND ELECTRONIC SECURITY CORE APPLICATIONS 8

MODE2 KNOWLEDGE IN STUDENT-CENTERED R&D 10

RESEARCH AND DEVELOPMENT IS INTEGRATED TO LEARNING WITHIN RIESCA 15

PART II - Methods for Evaluating and Developing Critical Systems 19

MODELLING, SIMULATION AND THE DEVELOPMENT OF CRITICAL INFRASTRUCTURES 21

A SERVICE DESIGN FRAMEWORK FOR ITIL 25

CONTINUITY MANAGEMENT MODEL FOR FINNISH SME'S: A DESIGN SCIENCE RESEARCH 47

IT CONTINUITY AND RISK MANAGEMENT OF CI 64

MATURITY-BASED CONTINUITY MANAGEMENT 68

SECURITY MANAGEMENT CO-OPERATION WITH AUTHORITIES AND LOCAL COMMUNITY OPERATIVES 112

BORDER SECURITY 113

THE CRITICAL MOBILE ICT SYSTEMS OF LAW ENFORCEMENT AUTHORITIES AND RESCUE SERVICES 116

PART III - Security of Critical Events 118

COMMUNICATION AND SECURITY MANAGEMENT CO-OPERATION IN LARGE EVENTS - CASE: IAAF WORLD CHAMPIONSHIPS 2005 IN HELSINKI 119

NUCLEAR SECURITY AT PUBLIC EVENTS AND POLITICAL MEETINGS 137

SCHOOL SHOOTINGS AND OTHER CRISIS SITUATIONS 140

List of Publications 143

Foreword

This report is the result of the RIESCA project (Rescuing of Intelligence and Electronic Security Core Applications), which serves as a 'toolbox'; a series of procedures for the evaluation and development of critical systems and the security management of events.

The report is divided into three Parts. Part I introduces the student centred R&D work and research methods used in the RIESCA project. The student-centric research and development work is integrated into learning as an actualisation instance of the Learning by Developing (LbD). The learning activities have shifted the focus of traditional teaching methods to learning by taking part in authentic R&D. In this way the students are participating in authentic R&D and they occupy the main active role in Laurea's collaborative R&D processes.

Parts II and III present the results of the student-centred R&D in the RIESCA project. Part II deals with methods for evaluating and developing systems that are critical for the functioning of Finnish society. Part III studies critical events (mass events, high level political meetings, crisis situation) and their security management and communication systems. The Parts are divided into Chapters that are classified according to the topics of Laurea's work package for RIESCA.

The outcomes of the student-centric section of the RIESCA project are mainly qualitative. The generally high level of the results indicates that student-centric R&D is a significant development for the field of pedagogy at universities of applied sciences. Among universities of applied sciences in Finland, Laurea produces the highest number of ECTS credits from R&D. In addition, the students' participation in publications, project preparation and even project management activities proves that they are central actors in Laurea's R&D operations.

The particular strengths of the student-centric model are related to equality, trust and the role of students as central actors and holders of responsibility. The used model maintains and supports open interaction through the operating environment it creates, its agility in responding to the needs of the environment, and the functionality of its management model. The recognised challenges in learning are related to the uniqueness of the actualisation; "the spirit and perspective of learning and teaching is unique".

Espoo in May 2010

Rauno Pirinen and Jyri Rajamäki

PART I
Introduction

The purpose of Part I is to present the RIESCA project and demonstrate why and how student centred R&D is applied in the project.

In their article, Hanna-Miina Sihvonen, Juha Knuuttila and Jyri Rajamäki introduce the RIESCA project. Ms Sihvonen was the project manager for the consortium, Lic.Sc. Knuuttila acted as the manager for Laurea's RIESCA work, and D.Sc. Rajamäki was the research work supervisor at Laurea.

Outi Kallioinen in her article describes Mode 2 knowledge which is a type of work-integrated research and learning that can provide a novel response to the increasing demand for education relevant to the global knowledge economy. In the interpretation of the Learning by Developing, Mode 1 knowledge refers to a conventional knowledge production method in line with the so called old paradigm; knowledge is produced and created in a researcher-oriented way within a specific discipline. This type of knowledge is mostly theoretical or experimental, hierarchical and static. The research problems are set and solved within a scientific community. Mode 2 knowledge is built through research and development work carried out in authentic contexts that use applications and services developed by collaborators. Then, students on a collaborative work term are faced with real world research agenda, scopes and problems, like those faced by practitioners and organisations in the normal course of events and practice.

Rauno Pirinen in his article describes the research framework used in the actualisations of the integrative studies in RIESCA. The perspective and integrative learning activities of RIESCA also address collaboration and foundation issues within the Finnish innovation system's co-creation processes. The student-centred approach is presented as evidence of the challenge of producing high valued competences and research activities that generate expertise (complements of Mode 2 and Mode 1 knowledge) in competence development and in the every day practice of the Master and Bachelor of Business Administration studies at Laurea University of Applied Sciences.

The actualisations of the studies are part of a larger innovation system value network, in which a single intervention is part of a larger network of transactions and international transformations related to the RIESCA project. In this actualisation almost all instances of strategies, agreements and objectives are managed using bottom-up and student-centred principles.

Chapter 1
RIESCA, Rescuing of Intelligence and Electronic Security Core Applications

Hanna-Miina Sihvonen, Juha Knuuttila & Jyri Rajamäki

RIESCA (Rescuing of Intelligence and Electronic Security Core Applications) project was a Tekes Safety and Security Programme funded project, which began on October 1st, 2007 and ended on March 31st, 2010. The Riesca project's focus areas were on the following Tekes Safety and Security Programme points:

- National safety and security covers items in the defence, boarder guard, police, first response and fire fighting as well as customs operations
- Industrial safety and security deals with full agenda of corporate needs and respective solutions

Finnish society is highly dependent on different critical information systems that support society. Business secrets, patient records and the credit card data of citizens, to name but a few, are kept in electronic form and it is obviously important that such information is kept confidential and protected from unauthorised access. Therefore, it is crucial that information systems and software applications function in the correct way in case of attempted hacking or human error. Successful hacking or even coffee spilt on a computer may result in a system not functioning as required.

There are a number of systems, such as railway and power, hydro-power and nuclear power stations, that are critical for the functioning of society in Finland. When assessing possible risks, it is only seldom taken into account that power, hydropower and nuclear power plants are critically dependent on the reliability and security of information systems. Information security is often enhanced by purchasing technical solutions without any systematic planning and knowledge of how to protect the different segments of the system. In this case, the risk is not only the investing of information security resources in the wrong targets but the fact that the unplanned integration of systems and the related information security components may even create new security risks. In consequence, systems that are critical for society may not work as they should.

The RIESCA project aimed to solve this problem. The research project developed information security management methods that can be used to ensure the proper functioning of critical systems in all circumstances. The research partners in the project are the University of Oulu, University of Eastern Finland

(formerly University of Kuopio), and Laurea University of Applied Sciences. The international research partners were Georgia State University, USA; J. Mack College of Business, USA;, the Department of Computer Information Systems, USA; the University of Arizona, USA; and The Central Information Technology Services Department (ZID) of the University of Innsbruck, Austria. The project also involved small to medium enterprises (SMEs), major industrial businesses and public authority partners. The project ran until the end of March 2010. The project's budget was over 950 000 EUR from 2007 to 2010.

University of Oulu

The work package of the University of Oulu aimed at developing a Corporate Governance (CG) approach to information security related to the critical information systems of society. In order to achieve that goal, the information security risks of critical systems were analysed and methods for applying and implementing security aspects were developed. During the RIESCA project, researchers from the University of Oulu performed joint research with other participating research organisations in analysing existing standards and frameworks, and evaluating their applicability for the safeguarding of critical information systems. The goal was to develop a method, applicable for managing critical information systems in-formation security by utilising, as widely as possible, existing methods and standards. The method was piloted in organisations participating in the project. The method was further developed based on the solutions produced in the project. The concrete result was a "tool box"; a series of information security practices, which are applicable to the safeguarding of critical information systems.

University of Kuopio

The work package of University of Kuopio aimed at developing methods for increasing the reliability of society's critical information systems. In order to achieve the goal, methods were analysed and developed for improving, implementing and measuring reliability from the perspective of both system providers and customers. Reliability engineering was implemented in software development whereas customers can use numerical reliability requirements when acquiring critical core software. Methods were piloted in participating organisations. A tangible result gained from the project was an approach with which both system providers and customers could measure and adjust a systems' reliability to an adequate level by taking into account the whole software process lifecycle.

Laurea University of Applied Sciences

The work package of Laurea aimed at developing further evaluation methods on systems that were critical to the functioning of the society. To reach that aim in the project, there was an analysis of the methods that evaluate these systems'

continual development. Special attention was given to moving from normal situation to crisis situations, and recovering from the crisis to a normal state. The other aim was to further develop different critical events (mass events, high level political meetings, crisis situation) security management and communication systems and assess methods for evaluating their functionality.

Chapter 2
Mode2 Knowledge in Student-Centered R&D

Outi Kallioinen

In the past few years there has been an increasing emphasis on starting to produce new knowledge in the networked communities of the universities of applied sciences in Finland. Laurea University of Applied Sciences in the greater Helsinki region is especially focused on creating longstanding value networks in the region. However, the co-creation of knowledge within the region is challenging and also a fairly new way to operate for a higher education institution. In order to fulfil this objective Laurea has been developing a new operating model for higher education pedagogy called, Learning by Developing (LbD), and has done so since 2000. In the LbD-model the integration of pedagogy, regional development and R&D is operationalised in an effective way so that the students as research colleagues play an essential role.

The OECD's theme for the analysis of higher education policy from 2006 onwards states that, as far as R&D is concerned, Finland has gained recognition throughout Europe for its innovative research activities and R&D strategies that particularly focus on the knowledge economy (Davies, et al. 2006). The national goal is to turn Finland into a world class leader in scientific and technological research, especially in applied research.

From the perspective of regional development, the OECD researchers highlights the fact that new knowledge is created in the context of the employment sector as well as at institutes of higher education, and that undergraduates should be placed at the heart of R&D activities. Referring to R&D at universities of applied sciences, Davies et al. (2006) mention Mode 2 knowledge production, which has a strong user-orientation and arises from genuine problem solving. According to the OECD study, the R&D activities of universities of applied sciences should specifically promote regional economic, social and cultural development. In this development the students' role is highly important.

The focus of the student and client orientation at Laurea specifically refers to the fact that the students are positioned at the centre of activity and that they are the most important interest group for Laurea. The realisation of this value was

notified in the assessment feedback provided by the Finnish Higher Education Evaluation Council, when Laurea was appointed as a Centre of Excellence in Education for the years 2005 and 2006 (Salminen & Kajaste 2005, 81) and as a Centre for Excellence in Regional Development for 2006-2007 (Käyhkö et al. 2006, 87). Only last November Laurea was nominated as a Centre of Excellence for student-centred R&D integrated into learning for 2010-2012 and in the feedback on FINHEEC (Kajaste et al. 2010).

The purpose of this 'reflective nutshell article' is to discuss Mode 2 knowledge production in student centred R&D in the universities of applied sciences. Students, at the core of R&D activities, create a pool of innovators, resources and actors that are needed in the transdisciplinary process of producing new knowledge, inventions, innovations and methods for the innovation environment and value networks. In the universities of applied sciences it is worth exploring the impact of Mode 2 knowledge (Gibbons, Limoges, Nowotny, Schwartzman, Scott & Trow 1994; Nowotny, Scott & Gibbons 2001; Scott 2005) on innovations platforms.

Mode 2 knowledge production allows operators to steer within universities of applied sciences when planning R&D processes for more participatory, dynamic and creative forums, which aim to result in the production of new competences. It is believed that transdisciplinarity, in particular, can produce something totally new – something which conventional disciplines cannot achieve.

According to Gibbons et al. (1994), the prerequisites for Mode 2 knowledge production are: (1) new technologies, rapid communication, virtual spaces for interaction and communication; (2) the crucial importance of communication and communication density, where expanding communication leads to a greater diversity of knowledge; (3) the possibility to utilise previous investments for knowledge infrastructure; (4) the expansion of higher education; (5) increased levels of communication and the use of new technology applications; and (6) the proliferation of sites with knowledge competences, whereby the knowledge surplus created supports the emergence of Mode 2.

Gibbons et al. (1994) characterise knowledge as follows: Mode 1 knowledge refers to a conventional knowledge production method in line with the so called old paradigm; knowledge is produced and created in a researcher-oriented way within a specific discipline. This type of knowledge is mostly theoretical or experimental, hierarchical and static. The research problems are set and solved within a scientific community.

MacLean, MacIntosh and Grant (2002, 191) state that the context of application in Mode 2 knowledge production means that the desired factor is to produce useful knowledge and competence in a pragmatic way, and that this is reflected when the research objectives, questions and practices are discussed in mutual

negotiations when setting up the projects. Mode 2 knowledge is produced (usually demanding participation by users) in the context of application. Knowledge is created in a transdisciplinary and multidisciplinary framework. Knowledge can be characterised as heterogeneous and heterarchical (organisational heterarchy), and is produced in social processes. Social accountability and/or responsibility, reflexivity and new forms of quality control are related to Mode 2 knowledge production, the five principles of Mode 2 knowledge are presented in following Table:

Mode 2 Knowledge	
1	context of application
2	transdisciplinarity
3	heterogeneity and organisational diversity
4	social accountability and reflexivity
5	quality control

Mode 2 does not carry the traditional meaning of 'applying knowledge to practice', where theory is tested and developed further by means of practical applications. Conceptually, application is closely linked with discovery, which brings about new perceptions, knowledge, innovation and competence. Thus, a clear-cut distinction between science and technology becomes increasingly difficult. This is evident in the creation of innovation; the competitiveness of the innovation system is challenged by models for both cooperation and competition between producers of new knowledge and competence (Gibbons et al. 1994). Mode 2 knowledge breaks the boundaries of conventional applied research and leads towards new competence and innovation, which cannot be foreseen at the start of the process.

The Mode 2 approach seeks to describe the way in which the ability of individuals and groups to create new things, transcends traditional boundaries, combines diverse sources of information and competence, and means the ability to innovate become increasingly important in the future (Novotny, Scott and Gibbons 2001). The essence of 'knowing' therefore changes from an act of remembering and repeating to an ability to find and utilise information. To this end, Jorgensen (2005, 51) strongly integrates a collaborative element, whereby utilising information, knowledge and competence together with others produces success, which at the same time creates social capital.

Mode 2 knowledge brings specific added value when developing applications for new innovations and producing new innovations. The study on knowledge crea-

tion by Nonaka and Takeuchi (1995) contains the same basic elements as Mode 2 knowledge; the abundance and density of interaction, knowledge processing and production among organisations and companies, and the shared ownership of knowledge.

In transdisciplinary problem solving MacLean et al. (2002, 191) argue that the skills of the participants are integrated within the framework of the activity, where interwoven empirical elements and a theoretical consensus arise and develop throughout the process as practical solutions and theory construction. These features cannot be distinctly categorised into certain disciplines. The results from the process are reflected and transferred to the subsequent activities of those involved in the project; this creates unpredictable dynamics, which are difficult to steer. This can be described as 'problem solving capability on the move'. Gibbons et al. (1994) summarise the four distinct features of transdisciplinarity:

Transdisciplinarity	
1	An evolving framework for problem solving, which steers endeavours for problem solving, i.e. issues are not finalised beforehand
2	A contribution to the knowledge: development of one's own theoretical structures, research methods and practices, which may not be applicable to a traditional scientific field
3	Knowledge is transferred and diffused during the production, which therefore demands participation. The results are circulated and developed faster in new problem solving situations than through professional journals or conferences
4	Transdisciplinarity consists of dynamic activity in which interaction networks are maintained by both official and unofficial means. The dynamic and changeable character of research makes it difficult to forecast new contexts of application

These prerequisites clearly emphasise the recent development and importance of information flow and management as well as the active utilisation of virtual possibilities, which form a clear distinction compared to knowledge generated by the traditional academic, theoretical research. However, Mode 1 and Mode 2 knowledge coexist, and Mode 2 knowledge develops from Mode 1 knowledge. Mode 2 knowledge production requires a theoretical basis constructed in multidisciplinary interaction. Without Mode 1 knowledge there cannot be true scientific new knowledge. At some point of the knowledge creation process Mode 1 and Mode 2 are intertwined. Mode 2 knowledge production is not the same as any experimental activity; it is a question of utilising research-based knowledge within a new type of mutual competence production process.

Universities of applied sciences have excellent possibilities to develop R&D activities in a way that brings Mode 2 knowledge and new competence production increasingly to the fore. The structures of research activities already exist, as does the need for working life transformation. Strengths include a high standard

of competence, close employer partnerships and most of all a flexibility regarding research activities. Networking is important for universities of applied sciences, which in itself promotes official and unofficial interaction channels that characterise Mode 2 knowledge. A potential challenge of Mode 2 knowledge production may involve its transdisciplinary approach; solutions are sought in unconventional ways by working cooperatively with actors that represent completely different starting points. The evolving framework for problem-solving and related unpredictable dynamics requires a readiness to change and, as far as the research process is concerned, an ability to operate and make decisions according to the situation. Further conflict may be caused by the creation of new R&D methods and practices that bring about new discoveries, which may not have a counterpart in the field of conventional science. Similarly, fail-proof criteria do not exist for evaluating the impact and reliability of Mode 2 knowledge. As a result, particular responsibility and ethical awareness become important in creating functional criteria and practices for evaluating Mode 2 knowledge as well as in applying current evaluation criteria for R&D project processes that produce Mode 2 knowledge. All these elements have a strong influence on the student-centred R&D process and call for the accountability of each participant.

References

Davies, J., Weko, T., Kim, L. & Thulstrup, E. 2006. Thematic Review of Tertiary Education. Finland. Country Note. OECD. Education and Training Policy Division.

Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P. & Trow, M. 1994. The new production of knowledge. The dynamics of science and research in contemporary societies. London: Sage.

Jorgensen, B. 2005. Education Reform for At-Risk Youth: A Social Capital Approach. International Journal of Sociology and Social Policy. Vol. 25, Number 8, pp. 49-69.

MacLean, D., MacIntosh, R. & Grant, S. 2002. Mode 2 Management Research. British Journal of Management, Vol. 13, pp. 189-207.

Nonaka, I. & Takeuchi, H. 1995. The Knowledge-Creating Company. How Japanese Companies Create the Dynamics of Innovation. New York: Oxford University Press.

Nowotny, H., Scott, P. & Gibbons, M. 2001. Re-thinking science: knowledge and the public in an age of uncertainty. Cambridge: Polity.

Salminen, H. & Kajaste, M. (ed).: Laatua, innovatiivisuutta ja proaktiivisuutta. Ammattikorkeakoulujen koulutuksen laatuyksiköt 2005–2006. Korkeakoulujen arviointineuvosto 3:2005. FINHEEC. Finnish Higher Education Evaluation Council.

Scott, P. 2005. Uusi tiedon tuotanto. Tiedepolitiikka 1/2005, 50-54. suom. Heli Mäntyranta.

Chapter 3
Research and Development is integrated to Learning within RIESCA

Rauno Pirinen

Student-Centred R&D Work is Integrated to Learning

The relationship between society and higher education institutions is changing; the higher education institutions are seen as an area for investment that can co-create research-based knowledge and added value in collaboration with an innovation system. This current change can be seen also in the reformation of the higher education field in Finland, for which this publication provides a sample of evidence of the actualisations of this new integrative paradigm, while giving a collected overview of integrative student-centred authentic research and development work in RIESCA.

Laurea's innovation of Learning by Developing (LbD) as a cultural framework and model of learning has been created in a social and collective process in 2002 - 2007. In recent years the focus of the LbD dimensions has shifted from a pedagogical orientation to authentic Research and Development work centred on students (the integration of learning and research), which means and has led to an inter-operative model in which student-centred learning is integrated within authentic and national and regional level research and development agendas and work.

Participation in the Centre of Excellence evaluation of education indicates that Laurea wants to further develop the student-centred R&D model (integrative research, development and learning culture) and subject it to constructive evaluation. Furthermore, Laurea wants to participate in the higher education and innovation discussion about the integration of learning and R&D, international activities and the leadership of higher education institutions.

Design Research

Different terms have been used to describe the most commonly used form of research in RIESCA, such as Design Research and Design Science Research (Hevner, March and Ram, 2004). Design Research (DR) consists of activities concerned with the construction and evaluation of technological artefacts to meet organisational needs as well as the development of their associated theories.

Consequently, design research is concerned with artificial rather than natural phenomena and is rooted as a discipline in the sciences of the artificial (March and Smith, 1995). Design Research is rooted in pragmatism in discussion (Haack, 1976). For the pragmatist, truth and utility are indistinguishable as truth lies in utility. For Design Research (DR), the relevance is evaluated by the utility provided to the organisation and developers. Thus DR must pass both the tests of science and practice (Markus, Majchrzak and Gasser, 2002). One set of guidelines for the conducting and evaluating of a DR is the seven elements of 'design research criteria' (Hevner et al., 2004).

DR makes a dual contribution to epistemic and practical utility. Any piece of research should add to existing theory in order to make a worthwhile scientific contribution and the research should assist in solving the practical problems of practitioners, specifically problems that are either current or anticipated. Two research methods in the information systems field with this dual orientation are Design Research (Hevner et al. 2004) and Action Research (AR) (Baskerville and Wood-Harper, 1998), which both take place in the student-centred RIESCA research cases.

DR consists of activities concerned with the construction and evaluation of technology artefacts to meet organisational needs as well as the development of their associated theories. In brief, behavioural science is concerned with theories that explain human or organisational behaviour, while DR is concerned with creating new and innovative artefacts (Hevner et al., 2004). The similarities of the fundamental characteristics of AR and DR are presented by Järvinen (2007).

In student-centred integrative learning and action different types of designs and development are integrated into an environment, practice and action. All sustainable AR phases include design e.g. economic design, service design, product design, system design and action design. Thus, AR (focus on change of actualization and organisation) is similar to but differs slightly from DR (focus on building, co-creating and evaluation) in view of integrative learning and action.

Action builds bridges from knowledge to competence and bridges design to the development and making of a commercial product, although this involves different processes, goals and theoretical assumptions. Integrative action connects an innovation system to these perspectives through the behavioural sciences i.e. psychological, sociological and educational; the focus is obviously on learning.

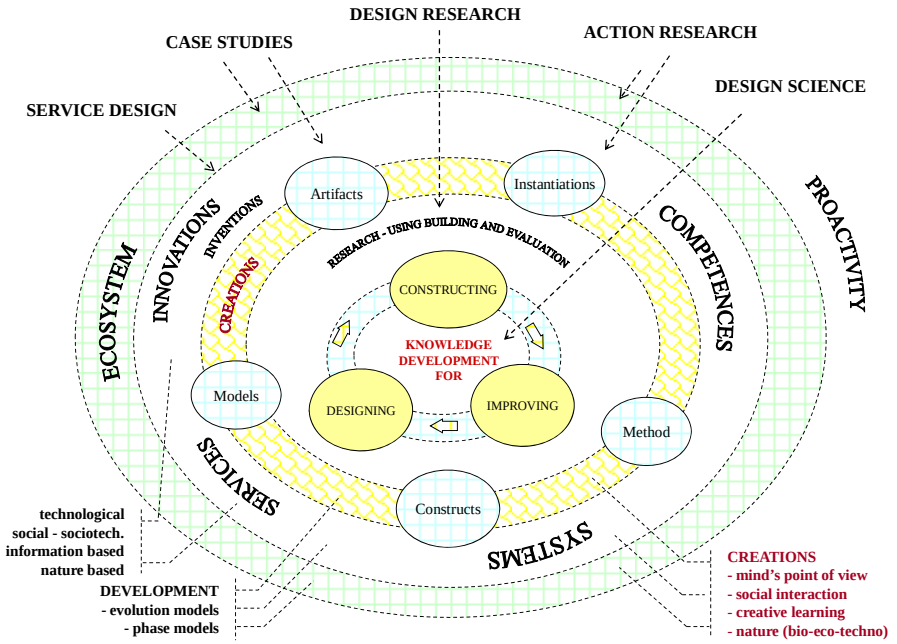
Service Design as Development Method

The earliest contributions of Service Design to the perspective of marketing and management disciplines are connected to Shostack's (1982) article "How to Design a Service". It describes the integrated design of material components,

namely products and immaterial components services. A design process can be documented and codified using a “service blueprint” to map the sequence of events in a service and its essential functions in an objective and explicit manner. Effective service marketing requires the recognition of the complex combination of products and services which make up a simple service (Shostack, 1982).

The Service Design Network was launched by Köln International School of Design in 2004. Currently, the international service design network (from the perspective of marketing and management) extends to service designers around the world, professional service design agencies and educational institutions such as Laurea. The Service Design of Information System in Integrative Action is mainly based on the Information Technology Infrastructure Library (ITIL v.3) and it describes Service Design’s principles, processes, technology related activities, tools, implementation and risks.

The framework of used methods is illustrated in following figure (proposed by Pirinen 2008):



Pirinen R. 2009. Research Framework of Integrative Action in America’s Conference on Information Systems (AMCIS 2009).

Action Research

The discipline of information systems is an appropriate field for the use of action research methods. Action research methods are clinical in nature according to Baskerville and Wood-Harper (1998) and Baskerville and Mayers (2004), and place researchers in co-operative and co-creative roles. Action research aims to solve current practical problems while expanding scientific knowledge. The action researcher's aim is to bring about organisational change while simultaneously studying the process. It is strongly oriented toward collaboration and change and involves both researchers and subjects.

In the RIESCA cases, action research is often iterative in scope and a continuous research process that capitalises on learning by both researchers and learners and expert participants in workplaces. It is a research method that places researchers and learners in a co-operative and co-creative role. In this environment, a theoretical genealogy of action research is based on "diversity in information systems action research methods" (Baskerville and Wood-Harper, 1998). Action Research assumes that a complex social process is best studied by introducing changes in that process and by observing their effects.

References

Baskerville, R., Myers, M. 2004, Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice – Foreword, MIS Quarterly, 28 (3), September 2004, pp. 329-335.

Baskerville, R., Wood-Harper, A. 1998. Diversity in information systems action research methods, European Journal of Information Systems (7), pp. 90-107.

Haack, S. 1976. The Pragmatist Theory of Truth, British Journal of Philosophical Science (27), pp 231-249

Hevner, A.R., March, S.T., Park, J., Ram, S. 2004. Design Science in Information Systems Research, MIS Quarterly (28:1), pp 75-105.

Järvinen, P. 2007. Action research is similar to Design Science, Quality & Quantity, 41, 2007, pp. 37-54.

March, S.T., Smith, G.F. 1995. Design and Natural Science Research on Information Technology, Decision Support Systems (15:4), pp 251-266.

Markus, M.L., Majchrzak, A., Gasser, L. 2002. A Design Theory for Systems That Support Emergent Knowledge Processes, MIS Quarterly (26:3), pp 179-212.

Pirinen, R. 2009. Research Framework of Integrative Action. Americas Conference on Information Systems (AMCIS 2009).

Shostack, L. 1982. How to design a Service, European Journal of Marketing, Bradford, Vol. 16, Issue 1, pp 49-64.

PART II
Methods for Evaluating and Developing Critical Systems

During the project Laurea's researchers and students, as research colleagues in co-operation with other RIESCA project researchers, analysed existing standards and methods. They evaluated their applicability for evaluation and development in critical system and event security management. The target of the project was to create a process for evaluating and developing security management during critical systems and events. This was done by making use of existing methods and standards whenever possible. The pilot projects on these methods were carried out, where possible, with organisations that took part in the project, although some pilot projects were executed with other organisations. The whole process (operations model) was supplemented with resolutions that were developed during this project.

Parts II and III present the results of student-centred R&D in the field of the RIESCA project including the abstracts of the student-centred journals, conference papers and several M.A. theses and some previously unpublished articles. The abstracts and articles are divided into Chapters according to the RIESCA work package topics.

Chapter 4 deals with modelling, simulation and developing the methods of critical infrastructures (CI) and contains four abstracts. Firstly, Pirinen and Rajamäki describe the RIESCA project and propose a new data collection and analysis model for CI evaluation as well as the creation of new evaluation methods. The second study is based on the first one and it (1) describes the RIESCA project; (2) proposes enhanced data mining collection and an analysis architecture model for critical systems evaluation; (3) includes a Business Continuing Management (BCM) method creation perspective for the context of critical systems and (4) describes RIESCA's action and process implementation model. It is not unusual that a critical system is connected to the Internet. Mikkola's thesis studies people's strong identification with certain web-services with regard to the finance sector. Several critical systems are entirely reliant on ICT systems; also the ICT supply process is crucial to critical systems. Nissilä's thesis designs, builds and evaluates new ICT supply processes. In Chapter 5, Helenius and Nissilä present this ICT supply process in more depth.

The security of supply in Finland is secured by a public-private partnership. More and more of the operators of critical infrastructures are small and medium size

entrepreneurs (SMEs). In Chapter 6, Noroviita and Uusitalo suggest a new continuity management model for SMEs. Chapter 7 studies IT continuity and the risk management of CI. Firstly, Arnell in his thesis creates an enterprise risk management policy for the Finnish Communications Regulatory Authority. The next two theses deal with the IT continuity management of large Finnish technology companies. Syrjänen describes an IT continuity management maturity model for a company that invests strongly in IT due to its high dependency on the availability of information systems. Lalla's case study describes how a newly merged global company managed to build a functional IT continuity management programme. Chapter 8 presents Syrjänen's action and design research on maturity-based IT continuity management.

National security consists of external and internal security and the protection of CI. Chapter 9 includes two theses that discuss internal security management cooperation with public organisations. An essential part of security work is cooperation with different authorities and local community operatives. Rusanen explores how security could be managed in state administration premises that have multiple tenant organisations representing different fields of state administration.

Chapter 10 investigates how new technologies and procedures could improve border security. Two studies carried out by Rajamäki, Turunen, Harju, Heikkilä, Hilakivi and Rusanen, deal with facial recognition systems (FRS); one dissects FRS as a maritime security tool, the other widens its context to airport security. Viitanen, Happonen, Patama and Rajamäki address the problems that law enforcement authorities (LEAs) encounter with regard to cross-border operations. The study explains how these differ from other operations and what kind of new procedures are needed.

Today, LEAs as well as fire and rescue services are increasingly dependent on mobile ICT systems. Chapter 11 includes three studies concerning this phenomenon. Two studies carried out by Rajamäki and Villemson; cover the designing of emergency vehicles' ICT integration solutions. The first study illustrates the operating environment and describes the main ICT systems of an emergency vehicle and presents a new mobile platform for a police car. The second study e.g. outlines a new service model that could be outsourced to 3rd party vendors and the methods that could be used to refine these models. Satellite tracking is one of the critical systems for LEAs. Kamppi's, Rajamäki's and Guinness' study covers the main satellite tracking system information security vulnerabilities and gives guidelines on how to make systems more secure.

Chapter 4
Modelling, Simulation and the Development of Critical Infrastructures

Modelling and Simulation of Critical Infrastructures Case: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA)

Rauno Pirinen and Jyri Rajamäki: In the Proceedings of the 2nd EUROPEAN COMPUTING CONFERENCE (ECC'08) Malta, September 11-13, 2008, ISSN: 1790-5109, ISBN: 978-960-474-002-4.

Abstract

According to the communication from the Commission to the Council and the European Parliament on Critical Infrastructure (CI) Protection in the Fight against Terrorism, CI includes energy installations and networks; communications and information technology; finance (banking, securities and investment); health care; food; water (dams, storage, treatment and networks); transport (airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems); the production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials);and government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

When assessing possible risks, it is only seldom taken into account that CI is critically dependent on the reliability and security of information systems. The Rescuing of Intelligence and Electronic Security Core Applications (RIESCA) project aims to offer constructive solutions to this problem. The research project will produce information security management methods that can be used to ensure the proper functioning of CI under varying circumstances. Furthermore, it will also lead to the development of a learning and laboratory environment for CI management and development.

This paper describes the RIESCA project and proposes a new data collection and analysis model for CI evaluation as well as the creation of new evaluation methods.

Rescuing of Intelligence and Electronic Security Core Applications (RIESCA)

Rauno Pirinen, Jyri Rajamäki, Lili Aunimo

WSEAS TRANSACTIONS on SYSTEMS. Volume 7, 2008 ISSN: 1109-2777.

Abstract

There are number of systems, such as transport and logistics, power and telecommunication, hydropower and nuclear power stations; that are critical systems for the functioning of the day-to-day life of society in Finland.

When assessing possible risks, it is only seldom taken into account that power, hydropower and nuclear power plants are critically dependent on the reliability and security of information systems. Information security is often enhanced by purchasing and extending technical solutions without considering any systematic planning and knowledge of how to protect the different segments of the system.

In this case study, the risk is not only considered with respect to poor investment in information security resources (i.e. the wrong targets) but also with regard to the actual increasing of risks through poor decision making. Poor decision making can result in the haphazard integration of systems, while their related information security components may even create new security risks.

As a result, systems that are critical for society may not work as they should. The Rescuing of Intelligence and Electronic Security Core Applications (RIESCA) project aims to find constructive solutions to this problem. The research object aims to produce information security and continuity management methods that can be used to ensure the proper functioning of critical systems under varying circumstances. Furthermore, it should also lead to the development of integrative action and an integrative environment for critical systems development, management and evaluation.

This study: (1) describes the RIESCA project; (2) proposes enhanced data mining collection and analysis architecture models for critical systems evaluation; (3) includes the Business Continuing Management (BCM) method creation perspective for the context of critical systems and (4) describes the RIESCA action and process implementation model.

An Individual's Strong Electronic Identification

Teija Mikkola

Master's Thesis, Laurea University of Applied Sciences, 2009.

The aim of this study is to clarify what an individual's strong identification in web-services is and when its use is necessary in web hosting. The most relevant strong identification methods used in Finland are described. One of the goals is to apply knowledge gathered in the T Group's online/web services. In the theory part of the study, the classification of web services, the authenticity of identification and the authenticity of the user identity are discussed.

There are many identification methods, such as the Tupas certification service offered by banks, the Katso ID offered by th eFinnish tax administration and Kela, and the Identity Card and mobile identification maintained by the Population Register Centre. In Finland, the most widely used and known identification method is the Tupas certification service. The benefit of it is that most of citizens already have a username and password.

The Ministry of Finance, The Government Information Security Management Board (VAHTI) has classified web services into seven main classes, according to their content and characteristics. These classes will help service providers to demand a uniform standard. The Identity Card project has not started as planned but there is strong need and wish to integrate people's identification methods. Finland's national policy and government bill promotes this project. So far the Tupas certification service has been useful, since it is widely used and known to be reliable.

New ICT Supply Process, Interfaces between Supply Process and the Project Management Process in the ITIL Service Design Framework

Marjo Nissilä

Master's Thesis, Laurea University of Applied Sciences, 2009.

The purpose of this work is to design, build and evaluate a new ICT Supply Process. The needs for developing the supply process are several. External partners, for example, expect the newest version of ITIL to be in common operation and also expect the existing supply process and project management process tasks to have identified any problems relating to dependency.

ITIL is the best known framework for ICT process maintenance and governance within the lifecycle of the initial system. Regardless of the Service Design materials shortcoming, the material is adequate enough to build a new ICT supply process.

ITIL Service Design does not include a supply process or phased project management process and only contains some relevant usable steps for various processes and levels.

The research question is: What kind of process is needed when purchasing ICT systems? The new version of the ICT supply process is based on ITIL Service Design version three.

The new process has been connected to the main support processes; the project management process and ITIL Service Design. During the work the leading role of the project management process was found when an external supply needed to be combined with development. In the new process the supply process is triggered by the project management process and the deliverables of the supply process are inputs to the project management process. To combine the phases of the process some major decision points have been added. The new ICT supply process is evaluated in theory against the two best process models. One is a process for public procurement and the other is a guide for non-specialist ICT purchasers.

Evaluation proves that the new ICT supply process is more than adequate. It fulfils most of the ITIL framework's valid criteria and most organisational needs. To achieve better results in IT projects, in 2009 only 32 % were successful (Galorath Incorporated 2008, 1), new ICT supply processes need to work as tools for IT projects.

The new process developed here should make purchasing more effective. Overlapping tasks have been identified and removed from the new process. Due to the fact that the new ICT supply process is based on existing processes, it will fit easily into the present environment. Implementing the new process alone without considering the required support processes is inadequate.

The research method is based on Design Research for Information Systems in which a researcher defines builds and evaluates in order to create something new and produce a new artefact. An alternative would have been Action Research but is better suited to further study on this work. The case study was at too early a stage from the point of view of this work.

Chapter 5
A Service Design Framework for ITIL

Kati Helenius and Marjo Nissilä

New ICT Supply Process, Interfaces between Supply Process and Project Management: a Design Research

This work focuses on the supply process for ICT systems including its phases. The work is based on ITIL version three Service Design. The four views described in Service Design are studied and the findings are presented as input material for the supply process development. The findings are expected to give input to improve and create more comprehensive ICT supply process. In general too little time is used to prepare ICT purchases. Often too little time is spent on preparation and monitoring and the evaluation of alternatives is often insignificant and preparation does not support decision making. In addition, targets are not set clearly and they are not connected properly to the strategy. In many ICT investments a decision based on the investment costs underestimates maintenance fees which often are many times higher than investment itself. Project management is needed to fill these holes in the ICT purchasing process. Project Management inherently includes tasks that the ICT purchasing process often lacks (Karvinen, Reponen & Vehviläinen 1994, 16-30). Standish Chaos Reports is probably the most referenced work on the issue and is adapted for Table 1. They define success as projects on budget and with expected functionality. Standish Chaos reports 2009 (Galorath Incorporated 2008, 1).

Functionality of ICT Projects	
Failed Projects	24 %
Challenged Projects	44 %
Successful Projects	32 %

Table 1: Expected functionality in projects

ITIL version 3 was published in 2007. Version 3 focuses on the cyclical governance model based on lifecycle management. Ten separate processes of ITIL V2 have been grouped and completed to create five approaches that include 26 processes in V3 (Introduction to ITIL 2006; Lloyd & Rubb 2007). This work focuses on the area of V3 Service Design, but extends to other areas when applicable.

The research method is based on Design Science Research for information systems (Hevner, March, Park & Ram 2004). In this work a new artefact is defined, built and evaluated. For the deliverable of this work – the new ICT supply process – the building phase laid out in the Design Science Research Guidelines by Hevner et al. is used and it is evaluated against two processes. One is the process for public procurement and the other is the guide for non-specialist ICT Purchasers. The criterion for evaluation is based on ITIL V3 Service Design and is made according to the relevant organisation.

Problem description and expected new results

There are several needs for developing the ICT supply process: external partners expect the latest version of ITIL in common operations, however, the new model of lifecycle management presents only a new version. Only a few parts of the supply process have been added to this new version and an overall picture of the requirements for the supply process is still lacking. Regardless of the shortcoming of the ITIL material, the material is adequate for building a new ICT supply process.

In the organisation's ICT supply process, the project management process tasks are only mentioned and no direct connections to either dependency are identified. Also, the roles responsible for the processes remain unconnected and the "leading" process for each step has been not recognised.

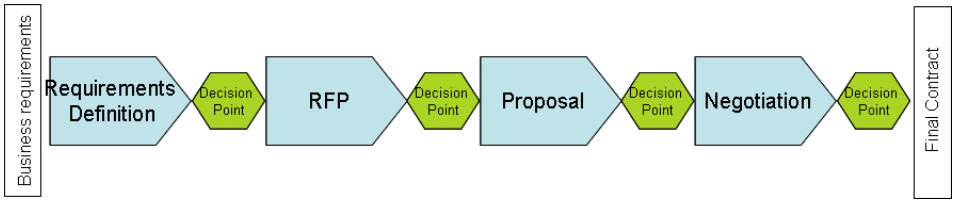
In order to get the supply process and the project management process to cooperate, a new process is needed. The connections and parallel flows of other processes, management and ITIL frameworks need to be described and assessed. More support processes are also needed for the ITIL framework processes. The tasks of these support processes include; requirement gathering, service catalogues and service level requirements, which provide key information or key inputs for the supply and project management process.

There is a gap in organisation between ITIL versions two and three. Due to this, not all the needed processes from the Service Design have been implemented yet and the processes have been developed independently at various times in different parts of the organisation. Further, the triggers for implementing the processes have had no direct connection. Within the Service Level Management the V3 process is split into three processes Service Catalogue Management and Supplier Management processes. In the organisation it is also clear that Information Security Management needs to be upgraded. Capacity Management and Availability Management in V2 and V3 are similar. There is no connection between the ICT supply process and any ITIL based process.

The expected result of the research work is that the new ICT supply process will fulfil the organisation's needs. The supply process and project management process phases, connections and dependences have been used as examples and from them it is obvious that the new process must have a framework from ITIL V3. Additionally, the new ICT supply process must fit into present environment.

Existing Supply Process

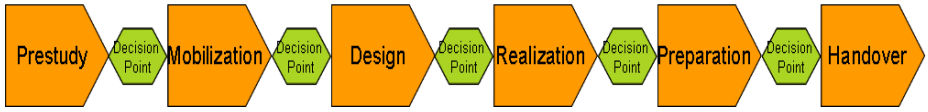
The supply process for an ICT system is triggered by business needs and is closed when the supply contract is signed. The process includes four main phases: Business requirement specification including a Request for Information (RFI) phase, Request for Proposal (RFP) phase, Proposal and Negotiation phases (Organisation 2007,). The decision points are located between the main phases.



Picture 1: Supply process

Connection of Supply Process to Project Management Process

The supply process and its phases include tasks, which are executed in the project management process. The project management process includes six main phases: Prestudy, Mobilisation, Design, Realisation, Preparation and Handover (Organisation 2005, 3-18). The first two phases are the most relevant for the supply processes.



Picture 2: Project management process

A business needs to react to various triggers from project management and then collecting the business requirements triggers the supply process. The prestudy phase of the project management process includes business requirement de-

termination, which triggers the supply process. The prestudy phase also produces a functional and technical conceptualisation of the supply process. When the supply process and mobilisation phase are finalised, the official project starts. The project team includes a project manager, representatives from businesses, technical departments, security and this involves experts on quality issues.

The Connection of the Supply Process to Existing ITIL Processes

ITIL processes have been under implementation for a long period and a few have been used for a long time. Implementations based on ITIL V3 are still ongoing. Simultaneously a need for upgrading the existing ones is already recognised.

The implemented processes are IT Financial Management, Service Level Management, Capacity Management, Availability Management, Change Management, Service Configuration Management, Release Management and Incident Management based on the ITIL V2. Access Management is being implemented according to ITIL V3. Service Continuity Management, Security Management and Problem Management are the next processes to be implemented.

ITIL as a Framework

ITIL (Information Technology Infrastructure Library) is a library, where best practices have been collected to improve an organisation's ability to advance at the same pace throughout all business sections and departments, and to find quality solutions to fit customers needs (Roos 2006, 3). It has not been standardised, but it has become the most widely accepted approach to IT Service Management in the world (Lloyd et al. 2007, viii).

ITIL is owned by the Office of Government Commerce (OGC). IT Service Management Forum (ITSMF) is the body responsible for the development (Introduction to ITIL 2006, vi-vii).

The original version of ITIL was developed at the same time and is in alignment with BS 15000, the former UK standard for IT Service Management. BS15000 was fast tracked in 2005 to become ISO/IEC 20000, the first international standard in ITSM. OGC is committed to the maintenance of alignment between future versions of ITIL and ISO/IEC 20000. (OGC 2009.)

ITIL version 3

In 2007 a new ITIL V3 was published. In this version, the perspective has moved from a process into focusing on service lifecycle thinking (IT Service Management Forum 2007, slide 10). ITIL V3 includes five stages, which are Service Strategy, Service Design, Service Transition, Service Operation, which all belonging to Continual Service Improvement (Lloyd et al. 2007, 6).

Service Strategy aligns business and IT and it ensures that every element of the Service Lifecycle is focused on customer outcomes. Service Transition provides guidance and process activities for the transition of services in the operational business environment. Service Operation introduces, explains and details delivery and control activities in order to achieve operational excellence on a day-to-day basis.

ITIL Service Design

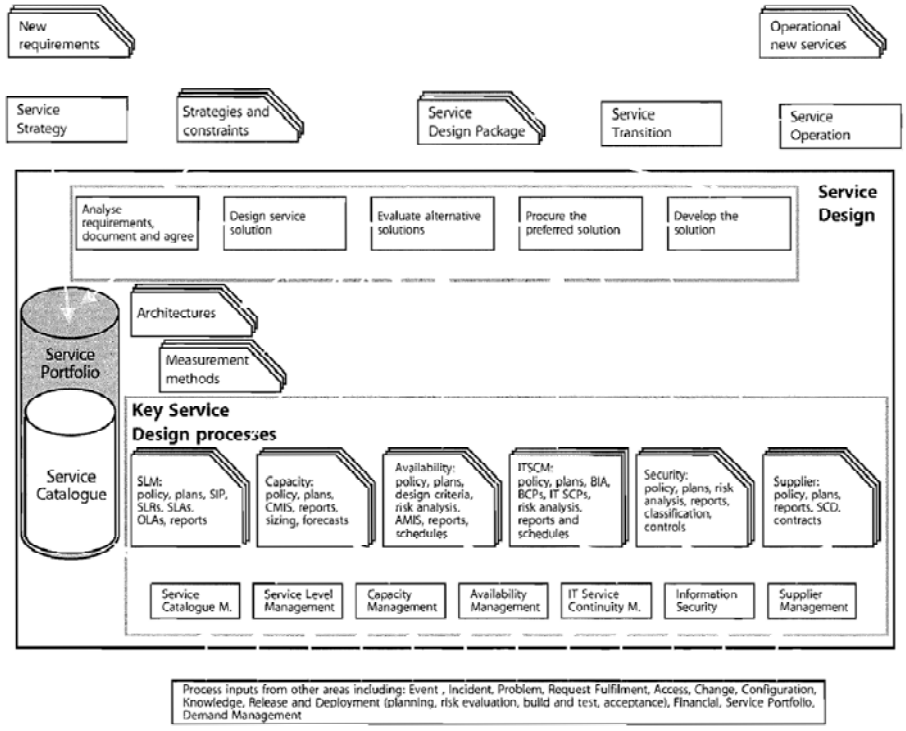
“A service is a means of delivering value to customers by facilitating ownership of specific cost and risks” (Lloyd et al. 2007, 11). The purpose of the Service Design stage is the design of new or changed services for production. In the design, it is fundamental, that all aspects and areas are covered and all activities and processes are integrated. In doing so, it is ensured that there will be only minimal issues arising during the subsequent stage (Lloyd et al. 2007, 30).

Service Design covers five aspects which are:

1. New or changed service
2. Service Management systems and tools
3. Technology architecture and management systems
4. The processes required
5. Measurement methods and metrics

The Service Design stage starts with a set of new or changed business requirements and ends with the development of a service solution to meet the documented needs of the business (Lloyd et al. 2007, 15).

Service design includes the designing of the solution and the development of the solution as in figure 3 (Lloyd et al. 2007, 60).



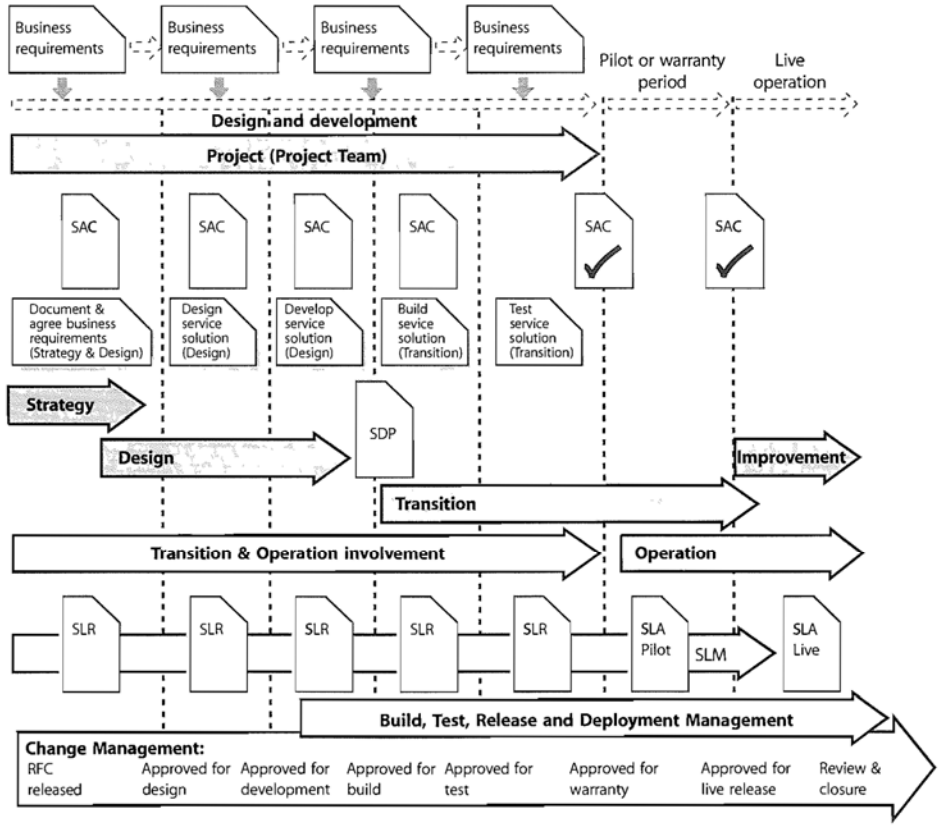
Picture 3: Service design – the big picture

Subsequent activities, the evaluation of the alternative solutions and the procurement of the preferred solution must be completed during the Service Design stage. One of the deliverables from design activities is ITT (Invitation to Tender) (Lloyd et al. 2007, 30, 46).

To enable the Service Design to get the needed information, the key supporting processes should be up and running (Lloyd et al. 2007, 59). In ITIL Service Design version 3 the processes are Service Level Management, Capacity Management, Availability Management, IT Service Continuity Management, Information Security Management, Supplier Management and Service Catalogue Management.

The project manager and the project team need to manage the stages from Strategy to Transition. The role is illustrated in Figure 4 (Lloyd et al. 2007, 31).

Project management is needed in the development stage, where service design is translated into a plan (Lloyd et al. 2007, 31, 47.)



Picture 4: Aligning new services to business requirements

Theory Related to ICT Purchasing

In general purchasing mean buying goods and services. It involves customer needs determination, supplier selection, arriving at a proper price, negotiating terms and conditions, signing a contract and following up the delivery (van Wheele 2005, 12). Goods are tangible, for example, raw materials or books. In contrast services are intangible, for example, software or licences (van Wheele 2005, 33). From this point of view the OECD (2009) defines ICT (Information Communication Technology) in the service category.

Supply issues must be considered as a process approach. A process includes steps and regards the steps as being connected. Moving from one step to an-

other must be completed with a decision after every step (van Wheele 2005, 28-29). Van Wheele (2005, 13) describes purchasing as a six phase function, the first three phases are specified as sourcing and the last three phases as supply. In this work the supply process correspond to how van Wheele describes the purchasing function, including phases from requirement determination to follow up tasks.

Van Wheele (2005, 224) defines the ICT support needed in purchasing as a database including articles, quotations and suppliers such as SAP. The focus is on buying goods which have, for example, codes and quantity. Nevertheless in many cases these database systems are still not capable of supporting the purchasing management so that required information is available. A shortage of overviews, vendor rating and purchasing performance reports for management are often lacking when purchasing transactional process supporting systems.

Van Wheele (2005, 33) notes that ICT licences and development contracts are purchased by a research and development manager. This does not mean that companies do not have departments for purchasing. It only shows that the agreed disciplines within a company are actively engaged in buying services.

Theory Related to IT Project Management

In general a project is work which is done for some unique purpose and to achieve defined results. A project has a defined goal, tasks and an outcome. It has start and end dates and a budget. In a project the allocated resources are combined with knowhow to achieve the target set (Organisation Oyj 2000, 2). The organisation is temporary and it will be wound up when its results have been achieved (Luomala et al. 2001, 10). Projects for businesses often need to include the knowhow to build an ICT system.

Phillips (2005, 328-329) defines the IT Project management process as including five phases: Project start, Planning, Delivery, Project Controlling and Ending the Project. The start and planning phases prepare the material for decision making. The supplier evaluation and the supplier selection take place during the project start phase (Phillips 2005, 196).

In IT projects Phillips (2005, 194-199) defines development purchasing as starting from identifying suitable suppliers. The next step is to shortlist two or three suppliers and to send out an RFP (Request for Proposal). External help for evaluating technical issues is recommended. Before signing a contract, reference calls and visits are recommended. Phillips (2005, 98, 115, 195) points out that the purchasing unit in an organisation buys licences but the IT project manager is responsible for purchasing the project development work.

Phillips (2005, 143, 233) recommends that ICT support tools such as the Microsoft Project should be used in IT projects. The tool can only support the project management process and it does not replace the need for project management, team leading or cost controlling. Project Management tools are very helpful when planning project tasks so that they fit into a limited schedule. A manager can easily see where more resources are needed or where reconstructive actions are needed. If general tools are used widely in an organisation then dependences on other projects can be recognised and handled if needed.

Research Preface

The philosophy in this work is pragmatism. It is a philosophical trend which emphasises actions and the relevance of practice also in perspective of science. Pragmatism tries to understand the present through the past. However, as a philosophy it is focused on the future. Philosophical pragmatists deny the correspondence notion of truth, proposing that truth is essentially what works in practice (Rorty 1982, 5).

March et al. (1992, 4) present Design Science Research as a method which attempts to create information technology based innovative things for people and their needs. A number of authors have used March and Smith's thoughts on science in their work such as Hevner et al. and Järvinen et al.

Design Science Research produces artefacts, models, methods and instantiations and includes two main activities; build and evaluate. March and Smith argue that an artefact must produce utility and the utility must be pointed out by criteria. The criteria must be generated from the artefact's environment as it will define how the artefact functions and how well it works (March et al. 1992, 4-5, 11, 16).

When research questions include verbs such as build, enhance, improve the scope of work then the research is probably within the scope of Design Science Research or Design Research (Järvinen et al. 2004, 103). Järvinen (2007, 1391, 1395) has noted that human and informational resources could be included in artefacts. This type of knowledge is used in this research work in a communication context. Järvinen (2007, 1394) also believes that artefacts should be evaluated against earlier best practices or example innovations.

The Design Science Research paradigm is proactive with respect to technology. It focuses on creating and evaluating innovative IT artefacts, which enable organisations to address important information-related tasks. The behavioural science research paradigm is reactive with respect to technology in the sense, that it takes technology as "given". It focuses on developing and justifying theories, which explain and predict phenomena related to the acquisition, implementation,

management and use of such technologies. Hevner et al. (2004, 98) argue that both Design Science and behavioural science paradigms are needed to ensure the relevance and effectiveness of IS research.

During this creative process, the Design Science Researcher must be aware of evolving both the design process and the design artefact as part of the research (Hevner et al. 2004, 78). Relatively little behavioural research has focused on evaluating models, which is a major focus of research in management science literature (Hevner et al. 2004, 77).

The problem of combining “real life” and a “scientific approach” is recognised as a challenge for this work, too. It is recognised that a lag exists between academic research and its adoption in industry. It also recognises the possible ad hoc nature of technology-oriented solutions developed in various industries. The latter gap can be reduced considerably by developing and framing the industrial solutions based on proposed guidelines (Hevner et al. 2004, 98). The artefacts constructed in Design Science Research are rarely full-grown information systems that are used in practice (Hevner et al. 2004, 83).

Hevner’s Guidelines

Design Science is inherently a problem solving process. The fundamental principle of Design Science Research from which seven guidelines (Hevner et al. 204, 83) are derived, is that knowledge and understanding about a design problem and its solution are acquired in the building and application of an artefact.

According to Hevner et al (2004), Design Science Research requires the creation of an innovative, purposeful artefact (Guideline 1) for a specific problem domain (Guideline 2). Because the artefact is "purposeful," it must yield utility for the specified problem. Hence, the thorough evaluation of the artefact is crucial (Guideline 3). Novelty is similarly crucial since the artefact must be "innovative," solving a hitherto unsolved problem or solving a known problem in a more effective or efficient manner (Guideline 4). In this way, Design Science Research is differentiated from the practice of design. The artefact itself must be rigorously defined, formally represented, coherent and internally consistent (Guideline 5). The process by which it is created and often the artefact itself, incorporates or enables a search process whereby a problem space is constructed and a mechanism posed or enacted to find an effective solution (Guideline 6). Finally, the results of the Design Science Research must be communicated effectively (Guideline 7) both to a technical audience (researchers who will extend them and practitioners who will implement them) and to a managerial audience (researchers who will study them in context and practitioners who will decide whether they should be implemented within their organisations).

Hevner's guidelines are adapted for Picture 5. The purpose of establishing these seven guidelines is to assist researchers, reviewers, editors and readers in understanding the requirements for effective Design Science Research (Hevner et al. 2004, 82-83.)

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Picture 5: Hevner's guidelines for Design Science Research

Used method: In this research, based on Design Science Research for information systems (Hevner et al. 2004), the researcher defines builds and evaluates in order to create something new; an artefact.

Process model method

Modelling techniques are used for the description of processes. The reason to use visual modelling is to make the process easy to understand, follow and teach to others. They are also a part of the documentation of the processes used to standardise, explain and make more visible the big picture of operations. Documents can be used as a part of any other processes, like quality documentation or training material. A good picture allows the easy understanding of material.

Diagrams, especially diagrams describing business processes and software systems, can become very complex (Harmon 2003, 91). The grouping is chosen to reflect the way a given company or group thinks about its processes and may vary from company to company. A process can be subdivided to any detailed level. The smallest process to picture in a process model is an activity. Many activities can be subdivided into smaller steps.

Processes are made up of sub processes and ultimately activities and linked together to produce organisational outputs. Processes describe the flow of work; functions represent the reporting relationship of the company (Harmon 2003, 109).

The process figure of the new ICT supply process uses standard objects to provide fast familiarisation. The main phases, for example high-level processes, are described within the pentagonal arrows. The decision points are shown as hexagons. Roles or parties are provided as titles and dividing lines. The start and finish are indicated through squares.

The New ICT Supply Process

The new version of the ICT supply process is based on ITIL Service Design V3. The input of deliverables to this work is the existing situation of the supply process in an organisation, together with the recognised needs of reengineering the process. The output of deliverables is then the revised version of the ICT supply process.

The proposed process model method is used for the presentation of new artefacts and the 7 step guideline was used as the process for creating the new artefact. The theory operates then as a framework for providing the deliverables and at the same time as the main framework to verify the scientific contribution. In addition, the new version has been evaluated and connected with the main supporting processes: The Project management process and ITIL Service Design.

The new ICT supply process was built by the authors Kati Helenius and Marjo Nissilä in the spring of 2009. The authors' research question was:

How can we connect the supply process and the project management process together with the relevant ITIL Service Design supply processes?

The authors used the existing tasks from the supply process and project management process and collected relevant tasks from Service Design to be added to the new ICT supply process. In order to understand how these processes are connected and how the tasks in different processes trigger each other and which

task is the leading one in any phase the authors created an analysis of steps in parallel processes. The leading tasks were found by finding the decision points and the owners of the processes. This is described in detail in Figure 6.

Process	Input	Phase	Description	Output	Decision point
Project Management Process	Business requirements determination	Prestudy	Gather adequate input for decision point of project initiation	Financial analysis Business needs and requirements Preliminary solution description Preliminary Technical roadmap	Common Decision point (decisions about project initiation and RFP)
Service Design/ITIL	Business needs	Analyze requirements	To define change, to document new functional and non functional requirements	Documented requirement	
Supply Process	Business requirements Preliminary supply proposal	Requirements definition	Collect and document business requirements for RFI	RFI	
Project Management Process	Go decision	Mobilization	Initiates project and prepares requisites for project launch	Project Plan Project organizatin Cost and benefit analysis Confirmed business requirements	Common Decision point (about contract)
Supply Process	RFI answers analysis Preliminary vendor evaluation	RFP	Collect and document materials for RFP Supply organization mobilization Receiving tenders	Supply plan RFP	Decision point for sending RFP
Service Design/ITIL	RFP	Design service solution (ext)	To define solution	Tender	
Supply Process	Tenders	Proposal	Evaluation tenders and create shortlist	Proposal for shortlist	Decision point for shortlist
Service Design/ITIL	Tenders	Eveluate alternative solutions	Evaluate solutions, vendors and score tenders. Proof of concep activities.	Proposal for shortlist	
Supply Process	Shortlist	Negotiation	To get better undestandig about proposed solution, terms, risks and price. Proof of concept	Proven solution concept Proposal for contract	
Service Design/ITIL	Decision of the contract	Procure the preferred solution	Finalize contract	Contract	
Project Management Process	Contract Proven solution concept	Design	To define solution	Update Project Plan Functional and technical solution description	Decision point (Aprove solution description)
Project Management Process	Functional and technical solution description	Realization	To build solution	Documented and tested system solution	Decision Point (Aprove solution and services)
Service Design/ITIL	Contract Proven solution concept Functional and technical solution description	Develop the solution	To build services	Documented and tested service solution	

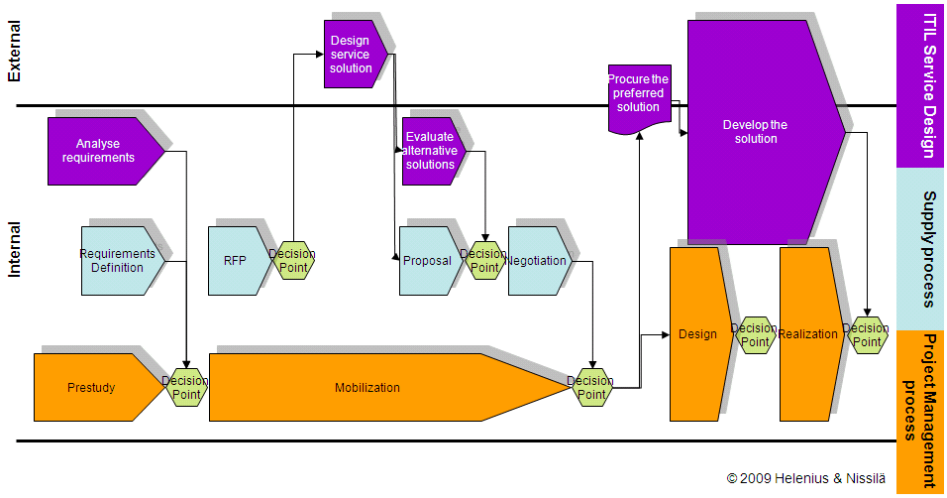
Picture 6: Analysis of steps in parallel processes

Based on the analysis of steps a new process was designed to give a common overview of how these processes are connected to each other as separate process flows. In the new ICT supply process (Figure 7) the parties are generically described in the left panel: external and internal, where the external is the vendor party.

The new ICT supply process was triggered by the project management process, which was triggered by a business decision. The project management process starts by gathering the business requirements, which provide the input for the first task of the supply process: requirement definition. The needs for the supply process are different though, as the input serves only the creation of RFI, compared with the needs of the project management process, but this does not justify the processes for separate requirement gathering.

The new ICT supply process deliverables are the inputs to the project management process design phase and Service Design procures the referred solution task. Compared with the existing supply process, where finalizing the contract was part of the negotiation phase, the task of procuring the solution has been transferred to Service Design.

The needed ITIL support processes are excluded from the new ICT supply process. This does not understate their necessity, as is presented in Figure 7.



Picture 7: The New Proposal of ICT Supply Process

The Evaluation of the New ICT Supply Process

The new ICT supply process is evaluated against two processes and their phases: process for public procurement and a guide for non-specialist ICT purchasers. The organisation uses government funds when purchasing and therefore must follow national procurement legislation. The guide for non-specialist ICT purchasers is aimed at business owners and managers who often see ICT as being a highly technical and specialised subject. The criteria for evaluation are based on the Service Design appendix C (Lloyd et al. 2007, 237). That provides a good basic list of the typical content of a process framework. On the other hand criteria are based on the organisational need to update the existing supply process.

The evaluation was conducted according to the Design Science Research static analysis method developed by Hevner et al. (2004, 86). In the evaluation of the New ICT supply process the methods of the case study, experiment, field study or simulation are excluded as evaluation methods. The theoretical evaluation is made from the customer's (internal) point of view.

In order to combine and analyse two other processes and the new ICT supply process similarities and differences and to draw conclusions, the researcher created a template for analysis (Yin 2009, 126-127).

The following abbreviations are used in Figure 8: PMP, Project Management Process, ITIL as ITIL Service Design and SP, Supply Process. On the left Accredit UK's (2008, 3) process for purchasing ICT is described. In the middle the new ICT supply process which describes the phases in the process is shown. On the right the open procedure process for public procurement is described (Aarla 2003, 1-3).

Guide to purchasing ICT: Phase	New Supply Process: Phase	Public procurement: Phase
Stage One - Plan the Purchase Stage Two - Detail your Requirements	Prestudy (PMP) Analyse requirements (ITIL) Requirements Definition (SP)	Planning of the procurement Publication of a prior information notice Setting up a specification and other substantive requirements
Stage Three - Identify Suppliers and Request a Quatation	Mobilization (PM) Request for Proposal (SP)	Invitation to submit Tenders Evaluation of the contents of tenders choosing the winning tender
	Design service solution (ITIL)	
Stage Four - Evaluate the Suppliers´Responses	Mobilization (PMP) Evaluate alternative solutions (ITIL) Proposal (SP)	Invitation to submit Tenders Evaluation of the contents of tenders choosing the winning tender
Stage Five - Select your Preferred Supplier	Mobilization (PMP) Negotiation (SP)	Invitation to submit Tenders Evaluation of the contents of tenders choosing the winning tender
Stage Six - Palce Ored with Supplier	Procure the preferred solution (ITIL)	Notification of the decision and the instructions for appeal conclude the Contract
Stage Seven - Implementation	Design (PMP) Develop the Solution (ITIL)	
Stage Seven - Implementation	Realization (PMP) Develop the Solution (ITIL)	

Picture 8: Evaluation processes

Results

Problem solved

An organisation's existing supply process needs a project management process. While analyzing an existing supply process the project management process tasks are only mentioned and in the project management process supply process tasks are also only mentioned. No direct connections to either dependency are identified. However, the latter project management phases like design and realisation need to connect and be combined with the supply process.

A project management process is always needed for development based purchased solutions but not for maintenance based purchased solutions. The importance of project management became clear during the evaluations, as did its leading role in the new process.

Some major decision points from existing processes related to the new process have been combined. Decision points were needed in order to situate the tasks of the supply process and separate the ITIL support into the phases of the project management process. The supply process connections are only a partial view of the service design deliverable process, as the supply process is always connected to a vendor party. Service design does not recognise parties, only roles and they are generic. In order to operate effectively the steering groups should also be aligned.

Service Design contains previous and subsequent phases compared to the supply process. During the work the researcher noticed that both the project management process and service design process are connected to subsequent phases. The basic deliverables of the supply process – a final contract with attachments – should have an addressee with a task to trigger the development phase. In the new process, it has been connected to the project management decision point. The governance for the purchase decision point is now handled by the project management.

The new ICT supply process uses only the deliverables of the project management process. In existing processes some tasks are carried out by the project management process and in the supply process. Requirement gathering is conducted in both processes.

During the evaluation, the new ICT supply process is more than adequate. It fulfils most of the ITIL framework's valid criteria and most of the organisation's needs. The new process includes six internal phases and one external phase. However, two other processes do not recognise the parties. Also no decision points were included in these two processes. All three processes start with a re-

quirement definition and purchase planning. Two of the models end when the implementation becomes finalised and one will end when a supplier makes a decision. Process measurements and metrics, tools and reports are not defined and included in the new ICT supply process in this work scope.

Excellence and ITIL

When going through the ITIL Service Design the author noticed that there was no integrated existing supply process and that only some relevant tasks existed. Tasks related only in theory were not considered to relate to each other as they had different hierarchical statuses in the processes. Also no decision points were included in the Service Design material.

Service design either ITIL does not contain a phased project management process. This work will be sent as a proposal to the owner of ITIL, OGC for the development of the next version of ITIL. The suggestions are described in more detail in the conclusions on the recognised ITIL development needs.

Challenges

All three models are processes and managed on a project basis. The new ICT supply process is based on ITIL. Although the ITIL process framework requires communication content in its process, Service Design does not have a tool or model to describe its process. Also all the process models lack communication and knowledge transformation.

The ITIL support processes are excluded from the new process. This does not understate their necessity. If any part of maintenance for the purchased solution is included in the contract – as it should be – the support processes need to evaluate, state in detail and plan to be up and running when they go live and the solution is executed. Tasks in these support processes are e.g. requirement gathering, service catalogues and service level requirements, which provide the key information or key input for supply and project management processes.

The supply process and the project management process roles and responsibilities must be synchronised and work effectively. In the existing supply process version, the business owner is responsible for the gathering of requirements, creating the business case, accepting the supply process team, the supply criteria and the commercial issues.

The supply process manager is responsible for the RFI process and the RFP process. The project manager of the project management process has no connection to the supply process. So the role of business owner is stronger in the

project management process but has the same individual operating in both processes.

Limitations

Process for the first phase of public procurement includes a definition for the method to be used in the process. In the new process, neither the prestudy phase nor the first phase of the guide for non specialist ICT Purchasers includes a definition.

The new ICT supply process will fit easily into the present environment. Implementing the new process alone without the needed supporting processes, process measurements and metrics, tools and reports is inadequate, though.

Conclusions

Improvements as a result of the new ICT supply process implementation

To achieve better results in IT projects the results of this work show that a new ICT supply process can be a tool. The first phases of project management; preparation and supply process and requirement definition have been combined with a common decision point. As Karvinen et al. (1994, 16-30) point out: too little time has been spent on preparing ICT purchases. Due to the combining, preparations have been synchronised. Project management helps cover for the faults of the supply process. IT project management includes tasks in setting the target (Phillips 2005, 11), defining a connection to company strategy (Phillips 2005, 76) and setting the budget including maintenance fees and follow-up tasks (Phillips 2005, 98-117).

The new ICT supply process is based on ITIL Service Design V3 (Lloyd et al. 2007). The ITIL framework does not contain any tools for the better two-way understanding for business and ICT people; only a high level approach of aligning is presented. Even so the use of ITIL terms provides a common terminology framework for ICT. The new process supports the need for common operations and models with suppliers. Also in the new ICT supply process both internal and external parties are defined and both parties process phases.

A result of implementing the new ICT supply process makes purchasing more effective. Overlapping tasks have been identified and extracted from the new process. The new process uses only the deliverables of the project management process. In existing processes some tasks for example requirement gathering to be carried out by the project management process and in the supply process. Effectiveness can also be achieved in resources. The business owner has many responsibilities in processes and by combining processes some operations such

as requirement gathering can be done only once. That does not however remove the need for requirement change management.

Recommended supportive actions in the purchasing field

The result of the evaluation of the new ICT supply process shows that implementing new ICT supply processes alone without the required supporting processes, process measurements and metrics, tools and reports is inadequate.

An organisation should have an information system to support the decentralised purchasing of ICT systems (van Wheele 2005, 241). This gives the possibility to coordinate all ICT purchasing activities. ICT systems usually lead to better discipline and more systematic communication from the purchasing operations. ICT systems also enable better management information and reports. As a result suppliers are better managed, due to the greater transparency of the purchasing operations. In generally an IT project uses ICT tools for gathering information through email, Excel, other Internet forms and Microsoft Project (Phillips 2004, 259-260). Organisations' should evaluate the possibilities to use these commonly used tools to support ICT purchases at organisational level.

In general processes should be measured and a process should have set metrics (Lloyd et al. 2007, 237). The main focus is to give information about process situation and development in clear and visual formats and point out if there are problems or improvements needed. A well defined and implemented measurement system gives a transparent picture of results and based on that it is easy to understand the connection between action and measurement. A universal, simple and practical model for measurement and metrics in purchasing is difficult to develop (Iloranta & Pajunen-Muhonen 2008, 434-444; van Wheele 2005, 250-267).

The new ICT supply process is managed on a project basis when supply and development is needed. In such cases IT project management measurements and metrics can be used. Phillips (2005, 13) defines budget, target and scope and a schedule as project metrics. A project needs a budget to illustrate how much money it is going to take to fulfil the set target. A clear and well defined target is the most important thing for a project - or that project will fail. The project schedule defines the time when the target is achieved and the project outcomes are ready to be transferred to the maintenance organisation.

In the new ICT supply process internal and external parties are described. In an organisation process the roles and responsibilities should be evaluated and distributed. The role of business owners is emphasised in a new process. Business units and their executives must take a leadership role in a handful of key ICT decisions. Unless business executives take responsibility for the success or fail-

ure of ICT purchases they will end up with systems that will have no impact on business. IT projects. Furthermore, departments should be held responsible for delivering solutions that are on time and on budget. Only business executives can make the organisational changes needed to generate business value from the new system (Karvinen et al. 1994, 120-123).

Recognized ITIL development needs for future work

Regardless of the shortcomings of the Service Design material, the material was adequate to build a new ICT supply process. No real supply process exists in Service Design - only relevant tasks. Subsequent activities, the evaluation of the alternative solutions and the procurement of the preferred solution must be completed during the Service Design stage. One of the deliverables from the design activities is ITT (Invitation to Tender) (Lloyd et al. 2007, 30, 46).

The process modelling method was chosen and used in this work (Harmon 2003), which includes techniques to describe the decision points of the new ICT supply process. Neither the ITIL generic process model (ITIL Service Support 2002, 273) nor the Service Design process framework (2007, 237) includes the decision points. In the ITIL process, the owner is responsible for ensuring that the process fits the purpose - but steering groups or comparable decision groups are not included.

The project manager and the project team need to manage the stages from strategy to transition. Also project management is needed in the development stage, where service design is turned into a plan (Lloyd et al. 2007, 31, 47). Tasks presented in the text were not shown in Picture 4. If a phased project management process exists in a company, it will need to be adjusted to an ITIL processes.

The ITIL framework does not contain any tools for an improved two-way understanding between business and ICT people, and only a high level approach to aligning is presented. Although the ITIL process framework requires communication content in its process (Lloyd et al. 2007, 237), Service Design does not describe it in its process. The use of ITIL terms provides a terminology framework for ICT with no focus on business people. For business discussions the terminology needs to be trained to the business party. For service level agreements a two-way understanding and communication support tool would prevent some problems from arising. Problems might develop if the service level targets are not aligned with business needs, or the ICT service provider activities and the service levels are not aligned with business expectations.

References

Aarla, T. 2003. Julkisten hankintojen hankintaprosessi. Kauppa- ja Teollisuusministeriö (Ministry of Employment and the Economy that started its operations as from 1 January 2008.). Referred 1.11.2009. http://www.aino.info/haku1/Hankintaprosessi.pdf

Accredit UK. 2008. Guide to Purchasing ICT: A Good Practice Guide for Small Businesses. Referred 1.11.2009. http://www.accredituk.com/documents/guidetopurchasingict-sme.pdf

Galorath Incorporated. 2008. Software Project Failure Costs Billions. Better Estimation & Planning Can Help. Referred 1.11.2009. http://www.galorath.com/wp/software-project-failure-costs-billions-better-estimation-planning-can-help.php

Harmon, P. 2003. Business process change. A manager's guide to improving, redesigning and automating processes. New York : Morgan Kaufmann Publishers New York.

Hevner, A., March, S., Park, J. & Ram, S. 2004. Design science in Information Systems Research. MIS Quarterly (28:1).

ITIL. 2006. Introduction to ITIL. 1. Edition. 3. Impression. London: The Stationary Office

ITIL. 2002. Service Support. 1. Edition. 6 Impression. London: The Stationary Office

Iloranta, K. & Pajunen-Muhonen, H. 2008. Hankintojen johtaminen. Jyväskylä: Gummerus Kirjapaino. 395, 390, 396.

IT Service Management Forum. 2007. ITIL V3 Roadshow. Uuden ITIL-version lanseeraustapahtuman esitykset. Referred 1.11.2009. http://www.itsmf.fi/?id=members&sid=arkisto

Järvinen, P. 2007 b. On_reviewing_results_of_design_research, Presented at the 15th European Conference on Information Systems

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Tampere: Opinpajan kirja.

Karvinen M., Reponen, T. & Vehviläinen, R. 1994. Tietotekniikkainvestoinnit. Jyväskylä: Gummerus.

Lloyd, V. & Rubb, C. 2007. ITIL Service Design. London: The Stationary Office.

Luomala, J., Heikkinen, J., Virkajärvi, K., Heikkilä, J., Karjalainen, A., Kivimäki, A., Käkölä, T., Uusitalo, O. & Lähdesvaara, H. 2001. Digitaalinen verkostotalous. Helsinki: Tekes. Referred 1.11.2009. http://users.jyu.fi/~timokk/tekes/digitaalinen_verkostotalous.pdf

March, S.T. & Smith, G.F. 1995. Design and Natural Science Research on Information Technology. Decision Support Systems. Vol. 15. No 4.

OECD International trade in services statistics. 2009. Referred 1.11.2009. http://stats.oecd.org/wbos/Index.aspx?datasetcode=TIS

Office of Government Commerce (OGC). 2009. ITIL. Referred 1.11.2009. OGC. http://www.ogc.gov.uk/guidance_itil.asp

Phillips, J. 2004. IT-projektihallinta sertifikaatti. Helsinki: Edita Publishing

Roos, A. 2006. ITIL- Siis anteeksi mitä? in Vätskäri 5/2009. Varsinais-Suomen tietojenkäsittely-yhdistys ry. Turku (Quint Wellington Redwood Oy). Referred 1.11.2009. http://ttlry-fi-bin.directo.fi/@Bin/b34c6627b00e604ae0c53c12482f9bf5/1231757204/application/pdf/1787002/vatskari_2006_5.pdf

Rorty, R. 1982. Consequences of Pragmatism, Minneapolis, MN: University of Minnesota Press

Sihvola, I. 2006. Onnistunut julkinen ICT-hankintaprosessi. Helsingin Kauppakorkeakoulu.

Van Weele, A. J. 2005. Purchasing & supply chain management: analysis, strategy, planning and practice. 4. edition. London : Thomson

Yin, R. K. 2009. Case Study Research - Design and Methods 4th ed. London: Sage Ltd.

Organization Oyj. 2007. Supply process. Referred 1.9.2009

Organization Oyj. 2005. IT Project Guide. 2 edition. 3. Referred 1.9.2009

Organization Oyj. 2000. Projektipäällikön projektityöohje. 3. Referred 1.11.2009

Chapter 6
Continuity Management Model for Finnish SME's: A Design Science Research

Heli Noroviita ja Katja Uusitalo

Introduction

The management of critical systems is no longer the sole responsibility of the public sector, but critical systems are also owned more and more by private companies. These private companies are also small and medium enterprises (SME), which have a significant role in society when we talk about the production of critical services. Thus, it is important to recognise the requirements of business continuity managements from the information systems point of view. In this article we introduce a Design Science Research project that is part of our M.A. programme studies in Information Systems at Laurea. The goal of the research was to create a model; an artefact, in order to manage the continuity of information systems in Finnish SMEs.

Our research problem was "What could be the proposal of the model for Finnish SMEs regarding Information System (IS) continuity management?". We identified the following three separate research questions:

1. How can we define a satisfactory level for a continuity plan for small and medium enterprises?

2. How can we utilise existing standards and operation models?

3. Is it possible to create an artefact which would be light enough and user-friendly and at the same time be assured that it will cover all the critical functions of continuity management?

Adaptation of the Research Methods

The Design Science Research method is used when new knowledge is created for design and implementation. According to Järvinen (2004), the Design Science Research method is used, when the research question includes the following verbs: build, strengthen, change, improve, extend. Design Science Research is technically oriented and adaptive (Järvinen, 2004).

March and Smith (1995) have discovered that an IS artefact is built in order to fulfill a specific task and after this artefact is built the research problem can then

be solved. According to Van Aken (2004) the mission of Design Science is to create new knowledge for the design and realisation of artefacts and new artefacts. In effect, a model, a method or a system that is better than the ones currently available. Van Aken (2004) also emphasises the usability evaluation of an innovation.

Alan Hevner (2004) has introduced into Design Science Research a framework, in which business requirements define a practical relevance for IS-research and where the knowledge base enables both the scientific and research viewpoint.

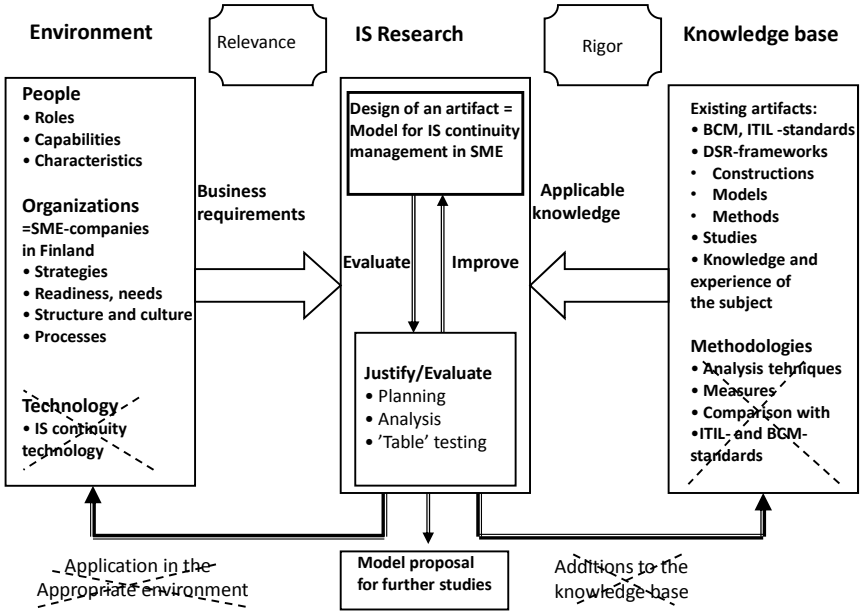


Figure 1: The adaptation of Hevner's IS research framework for our study.

In Figure 1 we show how we adapted our research plan with Hevner's IS research framework. We collected documentation regarding the subject from the scientific literature and from other sources. Our main sources were previous studies, literature and standards. Based on these sources, and the work we conducted in other study modules, we created our own proposal for the model. The evaluation part of the study is presented in a simple table. Based on the results of the first test round, we updated and improved the model. However, the model still needs further work and development before it can be implemented in a real world SME. In the following table we show how the seven steps of Hevner's (2004) Design Science Research guidelines were adapted for the study.

Table 1: Design Science Research Guidelines by Hevner

Design Science Research Guidelines		
Guideline	Description	Adaptation in our study
1 Design as an artefact	Design science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.	It is a simple, general model for continuity management in SME's, which does not currently exist.
2 Problem relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems.	Continuity management is an essential part of risk management in a company. The study looks for solutions to improve recognised problems.
3 Design evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.	A simple table testing was conducted during the study.
4 Research contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	.As a result of the study a preliminary model was created.
5 Research rigor	Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	The study method was based on the Design Science Research framework. Some of the references were taken from a scientific knowledge database.
6 Design as a search process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.	The search for a solution was focused on the needs of the Finnish SME companies.
7 Communication of research	Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	Results have been presented in the school community to the relevant teachers and students

Literature Study

IT Service Continuity management

Information systems are an essential part of business in all companies, even if the main industry of the business would not be information technology. IT plays an essential role e.g. in customer management, order handling, accounts payable and receivable and banking transactions. It is not possible to pass data security issues when information systems or IT services are handled. The diagram below illustrates how data security is an important part of a company's security. Continuity planning is part of the data security (Tietoturva ry, 2006).

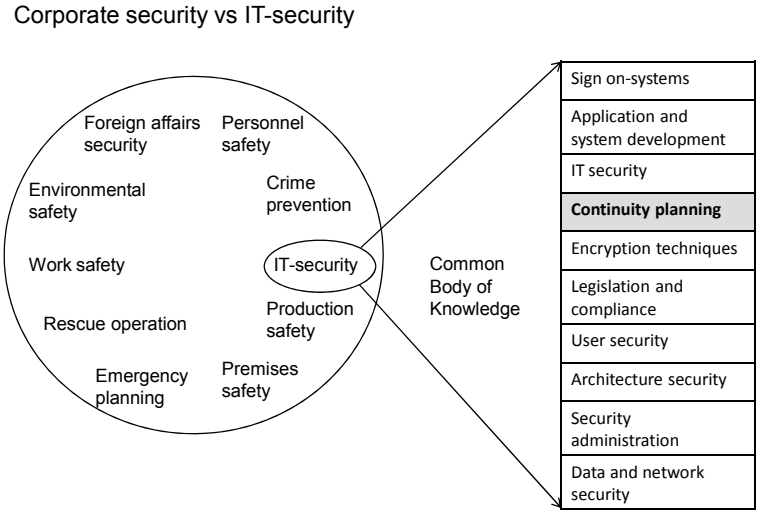


Figure 2: The tasks of data security as part of company security

The US Department of Commerce has its own specific standard Minimum Security Requirements for Federal Information and Information Systems in order to define a minimum level of data security requirements for the state's information systems. Though data security requirements for the state systems are partly higher than the requirements for the private sector the question remains; is the

United States' Federal IS security requirement listed also a good tool and checking list for private sector companies.

Continuity planning and the need for it have been defined in the abovementioned standard like this: "Organisations must create, manage and implement efficient plans for unexpected state of emergency. These plans must cover counter-measures, checking activities and return activities from state of emergency for IT-systems and –services. The purpose of these activities is to ensure that all critical information is possible to use and thus business continuity ensured."

In the instructions to the Finnish Financial supervisory authority it is emphasised that a recovery plan for IT services is the most important section of continuity planning. An essential issue of continuity planning is preparing for different crisis situations in the area of information technology. For crisis situations back up arrangements and a precise formulated recovery plan must be formulated. The alternative arrangements include the backing up of data, the duplication of critical equipment and components, the duplication of telecommunication connections, ensuring the undisturbed supply of electricity and substitute arrangements if people cannot participate. The recovery plans are usually written up in IT systems, and the plan should include sufficient detailed instructions about the action required to get an IT system or a part of an IT system up and running in varied crisis situations. The starting point for IS recovery planning is the estimation of the critical nature of the crisis and the required time for a return to normal operations. These estimates are created by the business units of the company involved (Rahoitustarkastuslaitos, verkkojulkaisu 2003).

In the handbook 'Is your company's information risk controlled?' there are example scenarios that make the importance of a security policy clear. The practical examples are given with regard to the continuity of a company's operations and the recovery from a crisis situation: The confidentiality, completeness and usability of information should be protected against threat and damage caused by defective equipment, software errors, natural disasters, conscious, negligent or accidental human action. These threats can be for example corporate spying against the company, other criminal actions, unmanaged publicity and information, privacy or data protection, the unintended leaking of information, negligence or carelessness when handling information. All these areas can incur damage and significant financial loss, hinder operations and damage functions (Teollisuus ja työnantajat, 2001, s.17).

Also mentioned are three examples that all emphasise the indispensable nature of IT service continuity planning. Since this is of consequence to all companies and organisations, in order to ensure their own competitiveness and existence during a state of emergency, the most important security issue to evaluate in every company is continuity management. Besides continuity management there

is the operational environment outside the company i.e. business networks. That is why managing the continuity of a company, guarantees the continuity of business partners in emergency situations. Thus, in agreement between companies there should be requirements for continuity planning. The agreements can include qualifiers for the partner to have continuity planning at an equivalent level.

Continuity management tasks

The main purpose of continuity management is to ensure that a company can operate under unusual conditions as planned. The minimum service level for unusual conditions must also be planned beforehand.

The British Business Continuity Management Standard, BS 25999, is an appreciated, well known and used standard that defines principles, processes and terminology for business continuity management. It is a collection of guidelines and recommendations that have been developed from best practices. It is possible to adapt this as standard in all kind of organisations no matter what their size or industry or company or organisation.

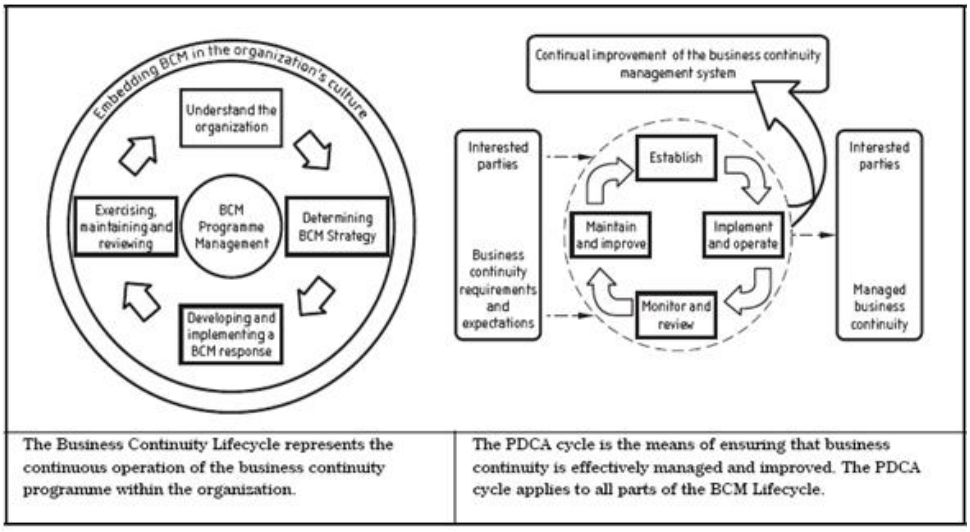


Figure 3: The business continuity management lifecycle (British Standard BS 25999)

In Figure 3 all essential elements of the BS 25999 standard are shown. Business continuity management must be have an ongoing cycle in an organisation. Continuity planning is not a onetime project. The core of the process is a continuity planning programme that consists of the following four parts:

An understanding of the business and organisation: Key products and services, critical activities and resources must be defined in the organisation. Business impact analysis (BIA) is part of this phase. The management evaluates the impact of losing resources for business (Doswell, 2000). Based on the results of the analysis it is possible to make decisions on how to minimise risks and ensure continuity.

Definition of continuity strategy: In the definition phase a strategy for a sufficient level of products and services during a state of emergency is chosen. The standard introduces the following issues for consideration: personnel, premises, technology, information, vendors and interest groups.

The development and implementation of a continuity plan: The framework of continuity planning is created. The framework will be implemented in the organisation. It will also define time limits for a sufficient return level.

The maintenance and re-evaluation of the plan: The standard emphasises regular testing, maintenance and follow-up of the continuity plan. As a result of the continuity planning the processes will be well tested and regularly maintained.

BS25999 introduces the PDCA-cycle to assure and improve continuity effectively. The cycle development is seen as a spiral, an endless process – after each round the target is one step nearer. The idea of the cycle is based on the idea of continuous learning. During the development spiral it is possible to check and change the final target. The phases of the cycle are introduced in the following table.

Table 2: The PDCA

PDCA	
PLAN	Define principles, goals, processes and guidelines in order to manage risks based on the principles in the organisation.
DO	Implementation of the agreed steps
CHECK	Follow and amend new operational models, processes and guidelines.
ACT	Maintain and improve business procedures according to the goals set by management. Implications for developing.

IT- service continuity management in SME's

Small and medium sized companies are companies which have less than 250 employees and a yearly maximum turnover below 50 million Euros, or whose grand total on the balance sheet is not more than 43 million Euros. It is also required that such companies are independent. Being independent means that companies are less than 25 % owned by large companies (Tilastokeskus 2008).

SMEs have more special challenges than large companies with respect to IT security. They have a specific role within IT services continuity management, according to the Ministry of Trade and Industry in Finland, which has done wide research on the level of IT security and IT risk management in SMEs. More than four thousand contact persons from various SMEs were interviewed. According to the research the issues that most need development were related to administrative IT security. This means the policies, planning, sourcing and responsibilities of IT security. Only 14 % of the companies had written an IT security plan and only 21 % had established a written IT security policy. Only 43 % of the companies had appointed an employee who would be responsible for IT-security issues (Pk-yritysten tietoturvakysely, 2006).

According to the research the most common reason for the failure of IT-security is a lack of knowledge and information, ignorance and non-proficiency. The other big reason was a lack of IT-security knowledge among entrepreneurs and management; also a personnel's lack of ability to use IT systems was a major problem. These were explained by the lack of resources in SMEs. All employees work with the core business and away from its support functions (Pk-yritysten tietoturvakysely 2006). Also, for management the outsourcing of IT-services has created the impression that someone else is taking care of all IT-related issues. However, the fact is that outsourcing changes the risk map in a company and it requires more input to update a continuity plan.

Security issues, like other essential issues in a company, have an impact on company culture. It is important for the management of an SME to be aware, that a flat organisation has the opportunity to implement changes and new operational models more easily because communication between company management, supervisors and employees is more natural.

Risk management and IT-security in Finnish SMEs are subjects which have recognized the need for development. Already in the 1990's at least two national projects were established: PK-RH, the Risk Management of SME's and its sister project PO-RISHA. The purpose of these projects was to improve risk management in SMEs by supporting SMEs and their employees and enabling them to forecast changes in the SMEs own operational environment.

The projects were executed by training the personnel and developing risk management methods. The personnel and management have a significant role in risk management issues. Risk management must be a conscious and continuous evaluation and improvement. The target of the projects mentioned above was to protect the vulnerability of SME-companies. (ESR-projektin loppuraportti, 1999).

As a result of the first phase in the project, a risk management tool set for SMEs was produced. This tool set included risk charts, checking lists, information packages, and guidance books. In the second phase a number of risk management web pages were published at www.pk-rh.fi. The content of the web pages was similar to the previous tool set. In addition new risk areas were covered, e.g. environmental risks and compliance management (Työterveyslaitoksen verkkolehti, 1999).

Web-pages are user friendly and free for everyone. They include several documents, listings, and other tools in the risk management area. From the IS continuity management point of view our first impression is that IT security related issues are just one minor part of the whole. Risks are classified per risk types and each should have its own folder. In these folders there should be several links to other subfolders and documents.

Risk types have been classified as follows: Business risks, Personnel risks, Agreement and liability risks, Information risks, Environmental risks, Project risks, Interruption risks, Crime risks and Fire risks. Different risk areas are handled together and there is a separate evaluation form that can be used as a support tool when evaluating and analysing risks.

The Results of Design Science Research

The Proposal of an IT Service Continuity Model for SMEs

When gathering and studying information about IT service continuity planning and during the creation of outlines for the proposal of a universal model for an IT continuity plan for Finnish SMEs, we ended up with the conclusion that the model can be at most a suggestive process description. In that process description all the crucial and most important tasks are presented. The result of this report is to propose a model which is intended to be adapted and taken into consideration for every company's own distinctive requirements. One of the main issues of the research questions remains open: Can it be assumed that SMEs have the necessary expertise to apply the model to their situation or should this model be more comprehensive and detailed? Is it a risk to have a model so generic and common that it gives great 'leeway' to those who will utilise it? Would it nevertheless be better to add to this model a very detailed instruction of every phase and the steps inside the phases? When working with this model we uti-

lised several references and previous reports which have covered the same theme.

In Figure 4 there are several issues that at least should be included in an SME enterprise's IT service continuity plan.

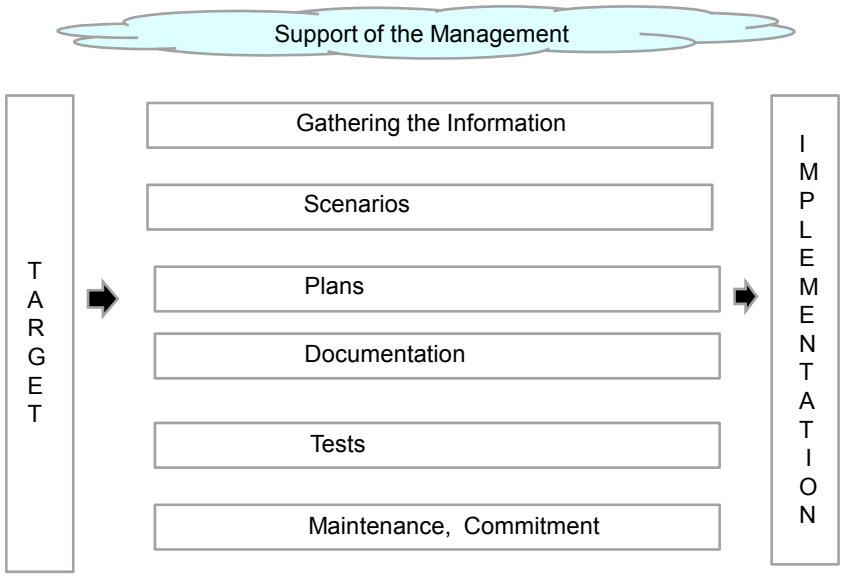


Figure 4: Proposal for the framework of an IT service continuity plan

The management of an SME should make the decision about the starting of a continuity management process and with that decision the management must make a commitment to the implementation of continuity process. If the management does not stand by this process, there is no likelihood of a successful and advantageous process. In this case the management should be aware of and take a conscious risk regarding operating loss, which can result from a threat or crisis situation.

A continuity management process includes the gathering of information and the creation of scenarios that involve threats. It must be noticed that these actions can vary extensively based on the company and business area. The gathered information is founded on the plan of the divisions of the continuity management.

After these actions the continuity plan should be thoroughly documented and tested. When the test phase is concluded the continuity process should proceed to a maintenance phase, which also has to be planned carefully. All the relevant personnel in the company must be trained and acquainted with the continuity plan and throughout the organisation there must be a common awareness of the continuity process and continuity plan. The commitment of personnel to the continuity plan is crucial if the implementation is to succeed.

Process model and the phases of the process

The continuity planning process can be divided into phases which are described in Figure 5. The actual process consists of these actions.

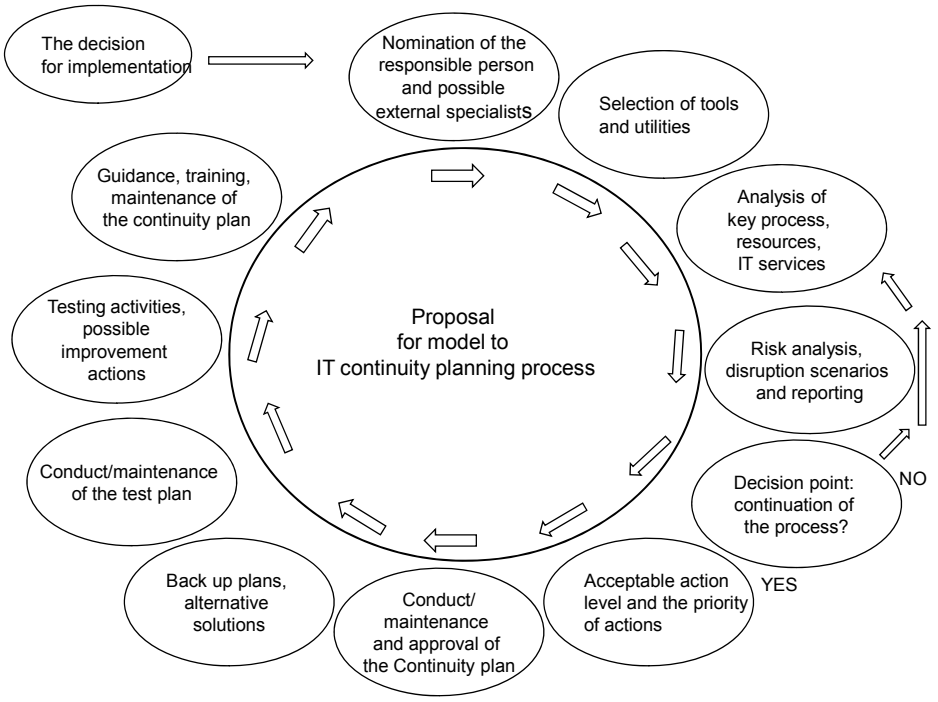


Figure 5: A model of the IT service continuity planning process

A model for the IT continuity planning process

The decision to start business continuity planning will come from the management of a company. In addition to the decision, the management must have an interest in and commitment to the continuity planning. IT service continuity plan-

ning is a part of business continuity planning, therefore when the management supports business continuity it also offers the required support for IT service continuity planning. It is essential that the management realise that the continuity planning process is a process which has to be constantly performed and always after extensive changes regarding the company. The continuity planning process should have at least one person responsible for it - in the same way other projects' or business processes' have. If the nominated person responsible in an SME has sufficient expertise he/she can coordinate and schedule the action of the process. The other option is that the person responsible will have the internal or external expertise to work with the process. To ensure the continuance of the continuity planning process the recommendation is that the person responsible be coordinated by a company internal resource. The tools, utilities, forms and metrics play a significant role in analysis phase and that they should have been selected beforehand. The selection of the tools for analysis may sound simpler than it is because there is wide range of different alternatives and a comparison cannot be made easily or rapidly. It is therefore appropriate to use the same tools and metrics in the following continuity planning rounds, which makes the comparison of results straightforward and the changes easy to find.

The analysis of key process, resources, IT services

The next phase in continuity planning process is to clarify the key processes and key resources of the company. In the SME this is phase is presumably quite easy to carry out because the core business, process owners and the other specialists are usually known throughout the whole organisation. When conducting a continuity planning for the first time a thorough investigation of the IT systems, the functionality and use of the IT systems and the connections of the IT systems to the business must be thoroughly carried out. These are topics that might require time and several internal and possible external specialists. If the maintenance and the development of the IT services are partly or totally outsourced, it is important to get an overview of the IT services. Also, it is beneficial to prepare companies for this phase through meetings and workshops with representatives of the outsourcing service provider.

Risk analysis, disruption scenarios and reporting

Risk analysis can be conducted by implementing the processes and using the resources. In the analysis phases all the risks, disruptions and threats that could cause a break in operation are identified and explored. This information forms the base for risk mapping, which happens by evaluating the probability of risk and its likely impacts on a company's business. The risks can be assessed by defining points about their probability and their likely business impact by using predetermined classifications or by trying to calculate the financial loss if the risk would actually occur. At this phase there can already be initial plans for every risk and how to prevent or mitigate those risks and their impact on company business. The results of a risk analysis and the disruption scenarios should then

be documented during the advanced stages of this phase. At the next decision point, which is the handling of the management, there should be a compact and unambiguous summary of the potential risks with information about the probability and consequence of the documented risks.

Decision point: continuation of process?

The most efficient way to present the work and the results of the action in the process so far is to have the person responsible for the continuity planning do it. He/she ought to have the best knowledge of the situation and the needs of business and also an understanding of the importance of the continuity planning to the company. The objective of the presentation is to get the management to internalise the significance of continuing the process and give a 'green light' to the next phases of process.

If the management do not want to continue this process or have the opinion that there is no significant risk to the operation of the company, the process will end at this point. The management will take either a conscious risk on the potential operating loss that could be caused by a threat or crisis situation or argue that they don't see any significant risks existing. If the process ends at this phase, the following round can be started directly from the analysis phase by analysing the business situation, resources and IT services. The following round can be agreed after a certain time period has elapsed e.g. one year, or after major changes in the organisation’s operation.

Acceptable action level and the priority of actions

To facilitate the continued handling of the continuity plan there is already during this phase a considerable amount of essential information from the previous phases of the process. There should also be the results of the analysis of the company’s business and IT services, risk analysis and interference scenarios, the prioritisations of the business action levels and their prioritisation and descriptions of the acceptable action level during a crisis situation. At a previous decision point the management of the company should have identified what the level and the intensity of the progress of continuity planning will be. In addition the phases that must meet with the management’s approval before moving to the next phase of process should be discussed. The practice is dependent on the commitment and the interest of the management and on how new the continuity process is. When the continuity planning is monitored for the first time in a company’s history it will probably feature highly motivated participants. In that situation the person responsible for the continuity planning process will certainly need as much help and support from the management and other interest groups as possible.

Back up plans and alternative solutions

At this phase the main objective is to identify and plan the backup arrangements and the instructions for any threat situation that might endanger the critical functions of the business. In the instructions there should be clear, complete advice on how to safeguard IT services, equipment, engine rooms and data communication connections. During the planning a company should pay attention to the different phases of a state of emergency:

- The situation right after the state of emergency occurs
- Action during the time when the crisis situation is occurring
- Recovering from a crisis situation and returning to a normal situation

In the backup plan there can be found a definition, who or what activates the In the backup plan there should be definitions of who or what activates the backup arrangements. The backup plan should include detailed instructions on how to start the backup action. When planning and evaluating the backup arrangements and the backup actions during the crisis situation all the possible alternatives should be estimated. From these alternatives the most feasible, reliable and cost efficient alternatives should be chosen. At this point of the process it is necessary to estimate the financial loss resulting from the crisis situation and compare it to the costs of alternative solutions.

An IT continuity plan usually covers restoring from back up media, parallel servers/environments, duplicating databases, alternative ways to take care of data communications among the other demanding issues which need high technical expertise. Based on those observations it is worthwhile preparing to use the help of external specialists in determining and forming a continuity plan.

The continuity plan should also contain alternative solutions for a crisis situation and a communication plan. The communication plan should be a simple list of contact information and the communication practice of the required persons and interest groups.

The Testing of IT service continuity

The best way to ensure that the continuity plan meets the defined requirements is to test it in practice. With this testing the functionality of separate fields should be tested. The purpose is to identify possible deficiencies and notice the need for development. In the test plan there should be goals set for the testing, test

methods, different phases of testing, how to make a realistic schedule and resource management plan and documentation. The testing should follow the designed plan, but during the testing there must be an evaluation of the extent of the tests. If it seems that the tests could be more comprehensive and effective than was planned then the original test plan should naturally be flexible and be able to be enhanced.

Guidance, training, and the maintenance of the continuity plan

When the continuity plan is ready and successfully tested, it will be published for the key persons of the continuity process. As there is no general advice about the breadth of the training and communication this must be planned case by case with the target groups, both internal in the SME and also externally. The aim of the training is to verify that all persons who are responsible for a company's IT systems and services are aware of the IT service continuity plan and are familiar with the content of the plan and they have clear instructions for the fault situation.

In the continuity plan there should be descriptions and collections of the backup plans and a communication plan, which should include contact information for every key person. The IT continuity plan is actually a practical instruction, a tool which must be used in a crisis situation. This is one of the reasons why the plan must be easily accessible for those responsible for it. On the other hand the plan includes confidential and sensitive business information and its confidentiality must be secured. The distribution of the continuity plan must be taken into particular consideration. In some cases it would be justifiable to split the continuity plan into smaller sections.

The maintenance of the continuity plan means that for an SME the objective is to ensure that the IT service continuity plan is always updated and up-to-date and that the plan is also developed. The IT service continuity plan is indisputably an essential part of the business continuity plan and risk management. The IT service continuity plan should be checked and, if needed, updated in the following change situations: organisation changes, changes in business structure, new business partner arrangements, a change of vendors, the deployment of new IT services and the alteration of crucial business processes.

The evaluation of the research method and implementation

The Science Design research method is well suited for this study. Using the Design Science frame work and the guideline with seven steps, both created by Hevner, we formulated a proposal for a model for IT service continuity planning for SMEs in crisis situations. This proposed model is a lighter and simpler version of the official continuity planning model, e.g. the ITIL standard. This model

is still an unfinished artefact, because this study did not include the validation of its functionality in a real world SME.

During this clarification process we completed a systematic test, after which we designed a proposal for an IT service continuity model for SMEs. During the model's testing and iterating, it changed and developed and the final documented model is the result of several rounds of iteration.

Conclusions and recommendations

The research problem includes three research questions which have been answered within this research process:

• How is it possible to define, to a satisfactory level, a continuity plan for small and medium enterprises? It is not possible to define one general satisfactory level for continuity planning outside of a company; instead the definition must be made for every individual continuity planning process case by case.

• How is it possible to utilise the existing standards and activity models? Using standards and existing standards and activity models it is possible to survey, identify and apply the crucial issues of continuity management. This requires expertise and ability in applying standards the ability to cover the topics in depth.

• Is it possible to create an artefact which would be light enough and user-friendly and yet provide all the critical functions of continuity management? Within this research there is no final answer to this question. The challenge is to make the standards simple and clear so that nothing relevant would be lacking. On the other hand the models must be and will be varied - depending on the business area and the size of the company.

The practical functionality of the model in an authentic environment must be tested and verified and that is the reason why this research is not finalised but needs additional research and testing. The testing should be implemented within several different Finnish SMEs and within various business areas.

References

Botha J. and Von Solms R. (2004), A cyclic approach to business continuity planning, Information management and Computer Security, Vol. 12, No 4, 328-337.

Business continuity management – Part 1: Code of practice, British Standards BS 25999-1:2006; Part 2: Specification, British Standards BS 25999-1:2007.

ESR-projektin loppuraportti, 1999,
http://esrlomake.mol.fi/esrprojekti/loppurap/lr960684.html, printed 14.5.2009.

Federal Information Processing Standards 200 (FIPS PUB 200), March 9 2006, Minimum Security Requirements for Federal Information and Information Systems, Department of Commerce, USA.

Hevner A.R., S.T. March, J. Park and S. Ram (2004), Design science in information systems research, MIS Quarterly 28, No 1, 75-105.

Järvinen, P. Artikkeli Onko innovaatioiden suunnittelu tiedettä (2006). Systeemityö, printed 14.3.2009,
http://www.pcuf.fi/sytyke/lehti/kirj/st20062/ST062.pdf.

Järvinen P. ja A. Järvinen (2004), Tutkimustyön menetelmistä, Opinpajan kirja, Tampere.

Kauppa- ja teollisuusministeriö, Pr-yritysten tietoturvakysely 2006, yhteenveto 8.2.2007,
http://julkaisurekisteri.ktm.fi/ktm_jur/ktmjur.nsf/all/E546D8A775141F0AC225727B003E0AE9/$file/Pk-yritystentietoturvakysely.pdf, printed 15.5.2009.

March, S.T. and Smith, G. Design and Natural Science Research on information Technology, Decision Support Systems(15:4), December 1995, pp 251-266.

Rahoitustarkastuslaitos, verkkojulkaisu 2003/03, Mitä tarkoitetaan jatkuvuussuunnittelulla?
http://www.rahoitustarkastus.fi/Fin/Tiedotus/Rata_tiedottaa/2003/3_2003/jatkuvuussuunnittelu.htm, printed 14.3.2009.

Teollisuuden ja työnantajain keskusliitto, 2001. Ovatko yrityksesi tietoriskit hallinnassa? http://www.ek.fi/ytnk08/fi/julkaisut_liitteet/Tietoturva.pdf

Työterveyslaitoksen verkkolehti, Työterveiset 1999, erikoisnumero: Toimivia työvälineitä pk-yritysten riskienhallintaan,
http://www.ttl.fi/Internet/Suomi/Tiedonvalitys/Verkkolehdet/Tyoterveiset/1999+Erikoisnumero/10.htm, printed 13.5.2009.

Van Aken J.P. (2004), management research based on the paradigm of the design sciences: the quest for field tested and grounded technological rules, Journal of Management Studies 41.

Chapter 7
IT Continuity and Risk Management of CI

Development of the Finnish Communications Regulatory Authority's Enterprise Risk Management

Jani Arnell

Master's Thesis, Laurea University of Applied Sciences, 2010.

The objective of this study was to generate an enterprise risk management (ERM) approach to protect the implementation of the strategic goals presented in the balanced scorecard of the Finnish Communications Regulatory Authority (FICORA) and to create an enterprise risk management policy. The practical section of the study was executed during 1st October 2008 – 15th November 2009. The theoretical section of the study explores the background of enterprise risk management in general and the theory of the action and constructive research methodology. The study was conducted partly as an action research and partly as a constructive study.

In the first phase of the study the writer built up an enterprise risk management approach to protect the achievement of the strategic goals presented in the target organisation's balanced score card 2009. The first part was conducted using communicative action research as a method, the results of which were used to generate an enterprise risk management approach. In the second section of the study a constructive method was used in which an enterprise risk management policy was generated. In the second section the writer became familiar with the regulatory environment of the target organisation, document archives related to enter-prise risk management and the results of the ERM self assessment executed in the target organisation previously. The writer also carried out benchmarking by exploring other organisations' and companies' enterprise risk management policies which were available on the web. Before the finalisation of the enterprise risk management policy of the target organisation it was introduced to a leading third party consultant to ensure that it would contain all the vital elements.

The overall results of the study showed that it was possible to successfully merge an enterprise's risk management and the balanced score card within the target organisation. This solution comes with benefits related to cost savings and scaling, which might be difficult to achieve in another way. By operating in this way, it is possible to obtain true added value from an enterprise's risk management as well, because ERM aims at protecting the main and the most valuable strategic goals of an organisation by using a familiar result-oriented manage-

ment method. By using such a method an ERM will also be less likely to drift away from the general management of an organisation.

The enterprise risk management policy integrates organisations' risk management efforts. When the organisation has implemented both the ERM framework and the method it is possible to compare results from different risk analyses performed in the organisation. With the help of ERM it has been possible to generate a common risk map at FICORA and enable interdivisional cooperation within the selection and implementation of organisation wide safeguards. ERM is one of the most valuable information sources for the situational awareness of an organisation. Exploitation of that situational awareness is an essential element of an organisation's success.

Maturity modelling as a catalyst for IT continuity management implementation in a large company

Kimmo Syrjänen

Master's Thesis, Laurea University of Applied Sciences, 2009.

This thesis will describe an IT continuity management maturity model and the concrete benefits this model has brought to a company and its IT unit. The organisation analysed is a large Finnish technology company that invests strongly in information technology due to high dependency on information systems availability. The role of business continuity and IT continuity management is to identify business requirements and provide solutions that ensure the continuity of information services and the capability to recover in case of disruptions or interruptions. Because of the large size of the target organisation and the considerably high number of information services, there is a need to implement target oriented and commonly accepted management models. This applies to IT continuity management processes and maturity models, too.

The target organisation developed and started to implement an IT continuity maturity model in 2007. The maturity model is a combination of business continuity, IT governance and information risk management standards and best practices built on top of commonly used process maturity models. This thesis will introduce the background and initial triggers for maturity model development. In addition, the maturity model's principles and usage cases will be reviewed.

The purpose of the study was to find out how much the IT continuity management maturity model has improved overall planning and the level of business continuity in the organisation studied. The core of this research is the evaluation, the purpose of which is to evaluate the concrete benefits the use of a maturity model has brought. The benefits will be analysed from five viewpoints: informa-

tion service management, IT line units, IT governance, corporate governance including risk management, and the point of view of the individual.

The evaluation is based on service quality reports, incident analyses and continuity reports. In addition to the extensive report base, open discussions and feedback from the IT continuity community has a significant role while assessing the maturity model value. The theoretical framework is mostly based on industry standards and best practices and the methods of canonical action research. Although the extensive source material provides a solid base for the research, the confidentiality of this information limits what and how much information can be shared in this thesis.

Building the foundations for information and communications technology continuity management in a merger based company

Markus Lalla

Master's Thesis, Laurea University of Applied Sciences, 2009.

This thesis case study report describes how a new global company managed to build the foundations for a functional IT continuity management programme and a framework for governance and resilience following a business operations merger of two major corporations. This involved the creation of an IT continuity management program, whereby the objectives were to analyse industry best practices and the maturity of the current process and to give recommendations on how to move forward in the event of key programme personnel not being available. The scope of case study is centred mainly on the beginning of the business continuity management programme lifecycle as defined in detail in the BS25999-1 standard. Therefore training and exercising are not discussed thoroughly.

This qualitative thesis begins with a description of the relationship between IT and business continuity management as well as the relevant terminology. For a company of any sort, it is important to collect immediate feedback on progress and to understand the reasons behind decision making, especially when two different business cultures are being merged. Data was collected through theme interviews, participant observation, and group discussions with various stakeholders and IT service management team members from IT services, who had been defined as crucial for the business. The methods used are also presented along with an assessment of their suitability for this study.

The thesis focuses primarily on general aspects of IT continuity capability design and current global trends in continuity management. The actual programme im-

plementation is not reported in detail due to the confidential nature of this work in practice. The thesis is of value mainly to me and the company. It is also a useful benchmarking case for any organisation with an obligation to ensure that enough IT recovery response controls are in place or planned to be implemented. Information about supplier chain risks caused by vendors and hosting partners who have a major role in IT continuity is also provided. Furthermore, it was discovered that internal dependencies and single point of failures extending beyond the core scope need to be monitored very carefully.

Chapter 8
Maturity-Based Continuity Management

Kimmo Syrjänen

Information Technology (IT) perspective on Maturity Modelling and Continuity Management: an Action and Design Research

This study describes an IT (Information Technology) continuity management maturity model and the concrete benefits this model has brought to a company and its IT unit. The target organisation is a large Finnish technology company that invests strongly in information technology due to its high dependency on information systems availability. The role of business continuity and IT continuity management is to identify business requirements and provide solutions that ensure the continuity of information services and capability to recover in case of disruptions or interruptions. The large size of the target organisation and the considerably high number of information services has led to the implementation of target oriented and commonly accepted management models. This applies to IT continuity management processes and maturity models as well.

The target organisation developed and started to implement an IT continuity maturity model in 2007. The maturity model is a combination of business continuity, IT governance and information risk management standards and best practices built on top of commonly used process maturity models. This study introduces and describes the background and initial triggers for maturity model development. In addition, maturity model principles and usage cases are reviewed.

The purpose of the study was to find out how much the IT continuity management maturity model has improved overall planning and the level of business continuity in the target organisation. The core of this research is the evaluation, the purpose of which is to evaluate the concrete benefits the use of the maturity model has brought. The benefits are analysed from five viewpoints: information service management, IT line units, IT governance, corporate governance including risk management, and the point of view of the individual.

The evaluation is based on service quality reports, incident analyses and continuity reports. In addition to the extensive report base, open discussions and feedback from the IT continuity community have a significant role while assessing the maturity model value. The theoretical framework is mostly based on industry standards and best practices and the methods of action research. Although the extensive source material provides a solid base for the research, the

confidentiality of this information limits what and how much information can be shared.

This study utilises the premises of design research and action research analysis methods that are institutionalised in the context of information system innovation and development. This work focuses on the supply process for ICT systems and their phases. The work is based on ITIL version three Service Design. The four views described in Service Design are inspected and the findings are brought as input material for the supply process development. The findings are expected to provide inputs to improve and create more a comprehensive ICT supply process.

Abbreviations

AirMiC	Association of insurance and risk Managers
AR	Action Research
BCM	Business Continuity Management
BCSC	Business Continuity Steering Committee
BS	British Standard
DR	Design Research
CMMI	Capability Maturity Model Integration
CoBIT	Control Objects for Information and related Technology
ICT	Information & Communication Technology
IEC	the International Electro technical Commission
IRM	Institute of Risk Management
ISO	the International Organisation for Standardization
IT	Information Technology
ITCM	Information Technology Continuity Management
ITIL	Information Technology Infrastructure Library
ITSCMM	Information Technology Services Capability Maturity Model
NFPA	National Fire Protection Association
PAS	Publicly Available Specification
PDCA	Plan, Do, Check, Act – model
RACI	Responsible, Accountable, Consulted & Informed
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOX	Sarbanes-Oxley Act

Risk and Continuity

Risk, by its very definition, always includes uncertainty about the severity of impact and probability as the risk may or may not actualise (Suominen 2003). Risks that have a higher impact on the organisation may require special atten-

tion. According to the Finnish Financial Supervisory Authority (FIN-FSA) operational risk management publication, financial institutes and organisations should regard continuity planning as an ongoing process and a natural part of their business operations and risk management. Business continuity planning in this context means preparations for interruptions in business activities so that the business can continue its operations and mitigate losses in various business disruptions. Disruptions may be due to damage to the employees, business premises, IT systems or data communications or intentional acts, water damage, fires or utility outages (Management of operational risk 4.4b 2004, 20-21).

The British Standard (BS) 31100 is a standard for risk management established by the British Standard Institute. It describes how to develop, implement and maintain effective risk management within a business by providing clear framework components as to how risk management governance should be arranged, what is a good policy, and processes and instructions on how to evaluate the outcome of the risk management framework used. The standard is aligned with several other risk management standards e.g. ISO 31000 (in preparation), Enterprise Risk Management COSO, and the risk management standard developed by the Institute of Risk Management (IRM) and the association of insurance and risk Managers (AirMiC). (BS 31100 2008).

BS 31100 (2008, 11) emphasises that, as part of the risk management function, there are specific risk areas where a detailed management or control framework is needed. Standards list the following as areas of specific risk management: Compliance risk, operational risk, health and safety, information security, and business continuity management. This Standard keeps information security and business continuity separate management entities for specific risk management purposes. What is interesting in the above standard is that it does not stress the role of IT as a separate risk management topic. IT, as it is understood as a larger function, is listed as a critical asset on several occasions and in all standards.

The British Standards Institution has published the Business Continuity Management standard BS 25999 which can be applied for various types and sizes of organisations. According to the standard, Business Continuity Management (BCM) is complementary to a risk management framework that sets out to understand the risks to operations or business, and the consequences of those risks. By focusing on the impact of disruption, organisations can recognise what needs to be done before any incident occurs and to protect its people, premises, technology, information, supply chain, stakeholders and reputation (BS 25999–1 2006).

According to Westerman and Hunter (2007), the first logical step in improving the foundation of the information risk management is to address availability risks. This can be done by addressing business continuity management as a

base for setting risk management in place. This powerful engine lays the ground work for managing at all layers of the 4As where the A means risks related to: availability, access, accuracy and agility. (Westerman & Hunter 2007, 60-68).

The examples above demonstrate that business continuity management is an important part of risk management practice. One can say that in order to extend an organisation's capability to manage the risks, which cannot be simply insured, transferred or compensated for by money, the implementation of business continuity management will secure an organisation's mission and continuity.

Business Continuity Management System

BS 25999 defines the business continuity management system as a business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework. A system should proactively improve an organisation's resilience against the disruption of its ability to achieve its key objectives. The basic assumption is that the system should include a rehearsed method of how to restore an organisation's key products and services to an agreed level within an agreed time after a disruption. So, as an end result, a business continuity management system may at its best deliver a proven capability to manage a business disruption and protect the organisation's reputation and brand against threats (BS 25999-1 2006, 6).

The ISO standard 21827 (2008, 117) for technology security capability maturity model refers to Dr. W. Edwards Deming's observation as follows:

"In a manufacturing plant, a manager observes problems with a certain production line. All he knew, though, was that people on the line make a lot of defective items. His first inclination might be to plead with the workers to work harder and faster. But instead, he collected data and plotted the percentage of defective items. The plot showed that the number of defective items and the variation from day to day were predictable." (ISO 21827 2008, 117).

Moen & Norman (2009) introduce the history of the PDCA model development. The PDCA model became well-known through W. Edwards Deming, although Deming called the model the Shewhart Cycle after its inventor and shape. It is also known as Deming's Wheel. Deming published the methodology in his book Out of Crisis (1982). He regarded the PDCA model as "a flow diagram for learning and for the improvement of a product and a process". The PDCA model corresponds to the general principle of managing a system according to general systems thinking, systems dynamics, or cybernetics. A modern application of the PDCA model is the Six Sigma methodology for an organisation's performance improvement (Brue 2002). Its most general activity phases are DMAIC – Define,

Measure, Analyse, Improve, and Control. As an example of another application area Figure 1 provides a comparison between the information technology service management ISO standard 20000 and BS 25999 business continuity management system standard. Snap shots (figure 1) of the given “Lifecycles” provide a good example of how the PDCA model is used in different contexts in business continuity and IT service management.

Even though the content of the lifecycles are different, both approaches highlight the importance of continuous improvement when using the key phases of the PDCA model. Both processes start with the planning and understanding of the current situation. The second phase is the execution of the plan by taking controlled steps after which one move on to the third phase; learning from the results. Checking the results provides the insight into which actions are needed in order to improve the process and, by that, to reach the optimum result.

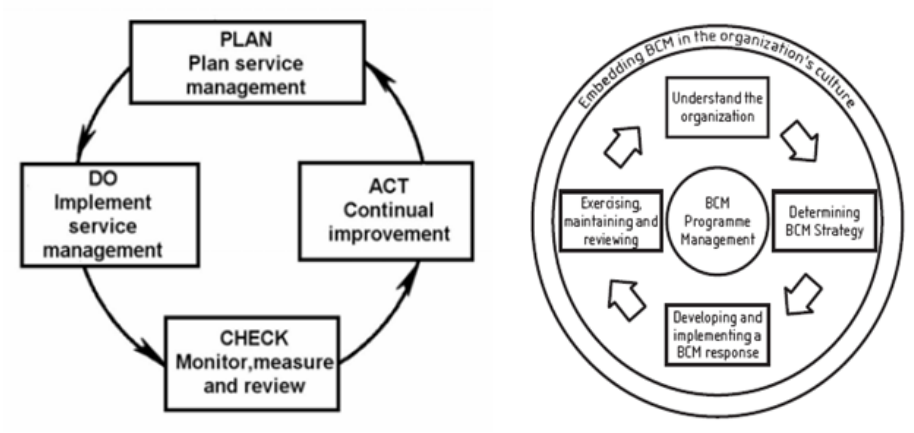


Figure 1: A Comparison of the Plan, Do, Check, Act model’s adaptations between the International Organisation for Standardisation and the International Electro Technical Commission (ISO/IEC) 20000 (2005, 5) and BS 25999-2 (2007, 3).

A consistent link to quality models enables BS 25999 to be integrated with related management systems standards, such as BS EN ISO 9001:2000 (Quality Management Systems), BS EN ISO 14001:2004 (Environmental Management Systems), BS ISO/IEC 27001:2005 (Information Security Management Systems) and BS ISO/IEC 20000:2005 (IT Service Management). (BS 25999-2 2007, 3).

Even though the standards provide common models agreed on by the different industry representatives and standardising bodies, it is important to keep in mind that each country’s standardising bodies and institutes often promote their own

approaches and this also applies to the BS 25999 as it is not the only standard related to business continuity management. When the number of available standards may start burdening the implementation, it is good to recap the ultimate goal of business continuity planning. Graham and Kaye (2006, 11) summarise the essence of business continuity management into four key points that apply to all relevant systems:

- BCM is not just about response, it is also about building resilience to strengthen an organisation
- BCM is not just about fighting fires, it is about understanding what might be at risk and developing strategies if things go wrong
- BCM is not just about having plans to recover a business that are over-elaborate, it is about having plans that suit the nature of your business
- BCM is not an extension to the business, and for it to be effective, it must be an embedded management process – as part of risk management, and in turn, as part of the business management (Graham & Kaye 2006, 11).

BCM "lifecycle" provides a solid structure for developing the business continuity management in organisations, whether private or public. Implementation of a high level management process as part of current organisation processes may become challenging, if it is not understood by those who should carry out the actual implementation. One way to solve this problem is to provide a tailored model of how business continuity management principles can be applied to in specific areas, such as information technology (IT).

Continuity Management

U.S. Federal information processing standard (FIBS PUB 87 1981) introduced the fundamentals of contingency and disaster recovery planning in automated data processing almost 30 years ago. At the time the standard development group identified the key topics that contingency planning should cover in order to have a working plan in case of adverse situations. The list below summarises the content of the FIBS PUB standard.

- Risk analysis and management's role in planning
- Preliminary planning scope, objectives and roles
- Preparatory actions related to people, critical assets, data and infrastructure

- An action plan for emergency response, backup operations and recovery, and
- Practice and exercises for testing the plan

Even then the FIBS Publication 87 emphasised that contingency planning should be an integral part of a programme for any data processing operation. As the standard continues, minor problems may become major and major problems may become catastrophic without a tested and effective plan on how to respond to and re-cover from unexpected and sudden disruptions of service (FIBS PUB 87 1981).

Since FIBS PUB 87, IT contingency and recovery planning has evolved into a managed process in which BS 25777 established by the British Standards Institution in 2008 represents the latest approach to IT continuity management. BS 25777 provides a common approach for information and communications technology (ICT) continuity management. The primary objective is to ensure that the organisation has plans in order to continue information and communications technology services at an acceptable predefined level in case incidents and disruptions should occur. The cornerstones for BS 25777 (2008, 3-4) are the six key principles for ICT continuity management:

1. Protect: Protecting the ICT environment from incidents, failures and disruptions by improving the resilience of ICT services
2. Detect: Detecting incidents at the earliest opportunity and minimising the impact on services
3. React: Reacting to an incident in the most appropriate manner will lead to a more efficient recovery and minimise any downtime
4. Recover: Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data
5. Operate: Running in ICT disaster recovery mode until a return to normal is possible
6. Return: Devising a strategy for every ICT continuity plan that allows an organisation to migrate back from ICT disaster recovery mode to a position where it can support normal business

As these six principles demonstrate, today's ICT continuity management is not only limited to response and recovery phases but is extended to cover also pre-work and actions for prolonged interruptions and for returning to normal operation. In order to promote the managed implementation of the given principles, BS 25777 applied BS 25999-1 business continuity management lifecycle model (figure 2). This model consists of six elements which should be implemented phase by phase starting with understanding business needs and moving from strategy determination to implementation and testing the strategy. The outer circle represents the implementation of continuity management into an organisation's culture.

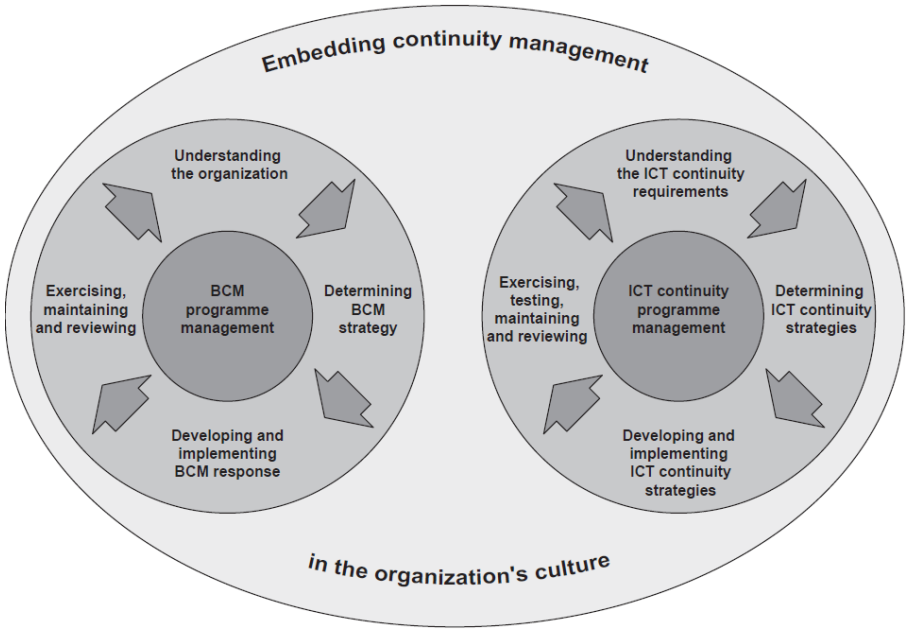


Figure 2: Relationship between ICT continuity management and business continuity management (BS 25777, 3)

The central governance element in both BS 25999 and BS 25777 is continuity programme management. The purpose of continuity programme management is to ensure ongoing development and implementation by steering all the planning phases consistently and in a goal-oriented manner. Goals and objectives should be carried out so that they fit an organisation's objectives as well as possible within the given timescales, resources and the budget.

BS 25777 (2008, 9) provides examples of what successful ICT continuity management programme should achieve:

- The ICT continuity management objectives should be clearly stated, understood and communicated
- Top management's commitment to ICT continuity management as part of business continuity management should be demonstrated
- Necessary resources should be allocated, and
- Those with ICT continuity management responsibilities should be competent at performing their roles

As the programme evolves and the organisation becomes more aware of the continuity management benefits it may become a part of the normal management process. In order to secure this change successfully it is imperative for the overall governance structure that a business continuity steering committee (BCSC) is appointed. The implementation of this steering committee ensures that an organisation's continuity plans are regularly considered, reviewed, tested, and updated when organisational change occurs. This group should be comprised of the most senior managers from the organisation and each key unit should be represented (BS 25999 -1 2007, 13-16).

Brue (2002, 36) refers to the famous William Thomson a.k.a. Lord Kelvin: "When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind. It may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science".

Brue (2002, 36) states that if you do not have measurements, you cannot make progress because you do not know where you are. This underlines the common management problem which also applies to business and IT continuity management, that is, how can we measure change? The continual monitoring of progress against an organisation's objectives ensures that actions and resources can be allocated accordingly. This can be done by having relevant and valid measurement methods that reveal issues and deviations on the process before they escalate into major problems. Basically, measuring change is one way to carry out risk management as the target is to predict and prevent incidents that would weaken the achievement of the business objectives.

BS 25999-1 (2006, 11) requires that a business continuity capability should be measured and BS 25999 part 2 specifications for business continuity management underline the importance of continual improvement based on objective measurement. U.S. National Fire Protection Association (NFPA) has created a standard for disaster, emergency and business continuity management. This NFPA 1600 standard (2007, 5) states that performance measurements should

be established and periodically reviewed as a part of continuity management programme. The problem is that this standard does not provide principles on what the performance indicators for successful programme management should be. From the continuity management point of view a common relevant and reliable measurement model would bring significant benefits when assessing an organisation's continuity capability, especially when managing large scale operations both in business and in IT.

Organization

The company studied (referred herein simply as the Company) operates in telecommunication globally. Because of its position, external expectations from shareholders and the Company community are relatively high, especially in matters of business continuity. The Company places a high priority on enforcing practice and exercises and controls balanced with informed risks, which will protect both shareholders' and the Company community's interests in the most optimal way.

The Company has a robust crisis management programme that has proven its effectiveness in real life situations; still, further development was seen necessary in order to be able to work more proactively to prevent risks. The corporate risk management unit started to formalise practice and exercises for business continuity management by collaborating with company security, infrastructure services and IT units. After exploring all relevant possibilities, the publicly available specification 56 (PAS 56 2005) was seen as a framework that could be best adapted into the current operation model for the Company. One reason for the selection was the fact that PAS 56 had a strong development community behind it and was linked to the respected British Standards Institution. Since then PAS 56 has evolved into BS 25999, which today is the globally recognised business continuity management standard.

The Company already had established risk, information security and crisis management policies when the business continuity management policy was under development. Business continuity management policy statements were embedded into other relevant management policies, as the objective was to keep the number of policies as low as possible. As a general guideline each business unit was responsible for ensuring business continuity in their own area at a level that fitted the mode of operation best. Since operations in a large organisation differ considerably from one business unit to another, the policy was written in a manner that allowed business continuity plans to be delivered in either a project or a programme mode. Delivering business continuity plans in a project mode was seen as beneficial for those units which had limited resources for a dedicated management system. The approach was especially successful in situations where fast actions were needed due to a sudden change of risk level e.g. pandemic outbreak, natural hazard, political restlessness or technological vulnerabilities.

The programme approach was seen best for situations where the business unit had a critical role in other company operations on a large scale. This role would set a high standard for maintaining a high preparedness and response level. When the scale of continuity planning increased inside the unit the continuity management programme provided an effective method to steer and control several planning streams at the same time. Continuity management programme subject matter expert's facilitated the planning process in order to make sure that plans were consistent and overlaps with other plans could be avoided. The continuity programme was seen as a first step in a process in which the long term objective was – and still is – to embed continuity management seamlessly into the organisation's normal operations and management.

Building the Continuity Management System

The initial step was to define and agree on the IT continuity management scope and relation to business continuity management. As a result, it was agreed that IT will take responsibility for all information services' continuity management, including the infrastructure such as data centres, network connectivity and IT personnel. This scope of the work resulted in business continuity management in which IT continuity plans are a subset for business continuity plans, allowing business units to focus on their response in case IT plans should fail.

The second phase was to define and agree on the level of implementation as that would affect the whole management concept. Basically it was question of which IT sub unit should act as the primus motor and who should take the responsibility for each system's continuity plans. As each IT service already had responsibility for the business requirement and information systems management, it was only natural to include IT service continuity planning as part of their role.

IT service and computer managers' role became critical for continuity management as they were responsible for managing the various applications' lifecycles and collecting requirements from business owners. To support IT managers and to ensure the consistent implementation of the IT continuity process, a team of continuity management specialists was established. The objective of the team was to develop the process and the tools, to provide training and consult when needed, to communicate common objectives and to follow the planning progress.

At the time PAS 56 provided the structure for continuity management but the terminology was seen as too confusing and vague for practical implementation in IT. In order to solve these problems the terminology and the model were modified in such a way that the user would better understand the given action and the main deliverables in each phase. Table 1 shows the changes between PAS 56 and the Company IT continuity planning model planning phases.

Comparison of Planning Phases	
PAS 56 (BS 25999)	IT continuity planning model
Understanding the organisation	IT Continuity risk and impact analysis
Determining BCM strategy	IT Continuity management strategy development and business approval
Developing and implementing BCM response	IT Continuity strategy deployment and plan delivery
Embedding BCM in the organisation's culture	IT Continuity plan communication and training
Exercising, maintaining and reviewing	Maintain & exercise IT Continuity Plan

Table 1: The comparison of BS 25999 and Company IT Continuity planning implementation

As the example above shows, the planning process included several phases. In order to ensure that continuity planners would understand that each phase needed to be completed before starting the next one, a simplified process flow was created (Attachment.1).

Continuity plan exercising was seen as the most important part of the process, so the PDCA lifecycle was integrated as a part of the whole process. Using the PDCA lifecycle the importance of continuous improvement by rehearsing and practising the plans became visible to the planners. It was also clear that information systems are under constant change pressure due to new business initiatives and mandatory configuration updates. This change pressure was covered in the process by adding a clear loopback from the continuity plan maintenance phase to the planning and creating phases at the beginning of the process. The overall objective for drawing a single IT continuity planning process was to enhance communication and steer the continuity planners' actions in a desired direction.

Continuity Maturity Model

IT continuity management can be part of either the business continuity management or the IT governance discipline, depending on how responsibilities are shared between the organisations. Regardless of the responsible entity, management needs to have information about progress and capability from the processes and other activities in order to be able to steer the organisation. For example, the British Standard for Information Technology Service Management (ISO/IEC 20000-1 2005, 6) states that the service provider shall apply suitable methods for monitoring and, where applicable, measurement of the service

management processes. These methods shall demonstrate the ability of the processes to achieve the planned results. From the Company's IT unit's continuity management point of view it was necessary to capture the current continuity planning status across the IT and be able to follow its progress. In order to build a working maturity model for IT continuity management and IT governance purposes the following expectations were set by the senior management after recognising and specifying the problem area to be researched:

- The model must be simple and easily understandable for those implementing the process
- Key performance indicators must be scalable with the organisation and measured subjects
- The model must support senior management decision making
- The model must direct actions so that users will understand what they are expected to achieve
- Key performance indicators must reveal changes in order to identify possible gaps and forthcoming issues
- The model should support the reward system and,
- Demonstrate the level of assurance of the organisation's ability to respond and react during events that cause an interruption or a disruption

In order to comply with industry standards and internal expectations, the need for a maturity model was obvious. For this purpose the IT continuity planning process model provided a foundation for creating maturity measurement. The planning process was translated into a roadmap for IT services system development as part of a standard planning cycle used by the IT. In practice this means that the IT service team could plan how to allocate resources between the 1st and the 2nd half of the year (Table 2). This approach allowed the IT services that manage several information systems with different service level requirements to set balanced continuity objectives between the business critical systems and the standard systems. The fundamental part of this model was the decision that the unit of maturity measurement was not the IT service or the team but the information system itself. The rationale for this approach was the fact that failures in the information systems would cause an interruption directly in the business process. Due to this direct dependency measuring the systems' resiliency and recovery capability was seen as more important than the organisation's capability to respond and work in a problem situation (Company IT Continuity management process 2007).

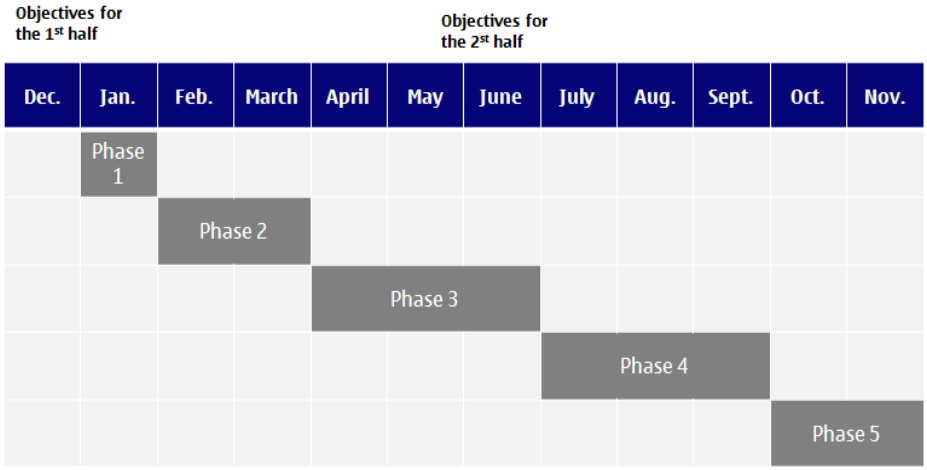


Table 2: An example of the common planning cycle showing how IT continuity planning phases are connected (Syrjänen 2009)

In order to ensure that each planning phase would be completed, a simple success criteria model was established based on the PAS 56 planning phases. The rule was that each criterion of success must be complete and validated by a continuity specialist team before the planning process could progress to the next phase (Company IT Continuity management process 2007).

The purpose of phase 1 is to build the rationale for why the continuity planning process must be initiated by conducting the business impact and risk analysis. The business impact analysis aims to identify and quantify impacts on a business if an interruption or a disruption should occur to its information systems. It is essential to understand and prioritise information about interdependencies between the business processes and systems. The outcomes of a business impact analysis are the recovery time objectives for the system and recovery point objectives for the data. Risk analysis aims to identify any operational risks which may cause extreme damage to the information systems which would then cause a failure or extended outage of the business operations. Based on the risk analysis findings and a business owner's risk tolerance a decision on further continuity development can be made (Company IT Continuity management process 2007).

The target of phase 2 is to identify available continuity solutions for an information system. When selecting the solutions, the costs to benefits calculation must be completed in a balanced manner. In this context balance means the cost of a

solution versus how effectively the solution can reduce the risk of failure or ensure a fast and controlled resumption of business. The final stage is to propose solutions to business owners and seek approval for the implementation for the one selected (Company IT Continuity management process 2007).

The success criteria of phase 3 contain two key actions, continuity solution building and documenting the IT continuity plan. Solution building is made according to standard project management and system development practices, and therefore this has not been defined separately. The criteria for the success are that the solution is implemented according to the risk and the business requirements and that the IT continuity plan document is available for validation by subject matter experts (Company IT Continuity management process 2007).

The target of phase 4 is to ensure that the plan is shared between all relevant teams and units; i.e. those who have a role in continuity solution management and the possible recovery actions, if it is necessary to invoke the IT continuity plan. This phase also includes IT service team training for the IT continuity plan use so that each team member understands their role and the role of other team members in case there is a need to initiate recovery and restoration actions (Company IT Continuity management process 2007).

Phase 5 demonstrates whether the continuity solution and agreed recovery actions will work as planned. The term technical exercise is used here as it combines both the crisis management and technical capability testing. Even though practice and exercise methods vary, depending on the solution in use, all of these practices aim to validate whether response, recovery and restoration can be done within the time targets set by the business (Company IT Continuity management process 2007).

As remarked earlier, the continuous improvement of continuity management was based on information systems' IT service teams constantly conducting practice of a technical nature. Successful technical practices provide evidence of the ability to recovery and restore information systems and data if needed. The result given by the Company demonstrated the highest level of assurance of mitigated risks and, by that, justified retaining the maturity level 5 (Company IT Continuity management process 2007).

Failures in the technical exercises and practices revealed weaknesses and deviations that would require special attention leading to corrective actions and dropping the maturity level down the scale e.g. a technical exercise might reveal that a back up process did not work promptly due to a technical mismatch. This finding would initiate the reconfiguration of the back up process that would be done at maturity phase 3. Even though a technical exercise is normally required for maintaining the highest maturity level, there is one exception. If the continuity solution has worked as planned during a real incident, the technical exercise

does not need to be completed. This is regarded as proof of a working solution; therefore the maturity level can be kept on level 5 until the next review round (Company IT Continuity management process 2007).

The model has now been used for three years and it is time to analyse and reflect on how well original expectations were met. According to Järvinen & Järvinen (2004, 103) scientific research can be divided into two main areas, basic research and applied research. The objective of basic research is to observe and analyse an environment in order to create and test new theories. Applied research uses results from basic research as scientific foundation to create new innovations for everyday use. According to Pirinen (2009, 10), the diversity of ways to generate innovation is huge and the nature of innovation generation is multidisciplinary. Pirinen provides a concept of six perspectives on research and development in integrative action (integration of research and development in education) which are not exclusive and all of which are needed to successfully consider processes of integrative action. This concept sets the framework for the following two chapters, which will reflect the journey of the IT continuity maturity model innovation in the context of Design Research and action research.

Design Research and IT Continuity Maturity Model

The aim of Design Research (DR) is to solve identified problems by delivering practical solutions and innovations (artefacts). An additional target is to provide new information for solving problems in the future. To decide whether the IT continuity maturity model belongs in the premise of DR, one must understand the concept of an artefact.

According to Hevner, March, Park & Ram (2004) both DR and the behavioural sciences are inseparable as technology and behaviour are not dichotomous in an information system. The fundamental idea lies on the fact that information system research is always at a confluence of people, organisations and technology, so it is more than a product. Based on this, IT artefacts can be defined broadly as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices) and instantiations (implemented and prototype systems).

IT artefacts are implemented in an organisational context i.e. information systems are for people and organisations, not an end in itself. This is the rationale for the object of study in information systems behavioural science research. Behavioural sciences research objective is to predict or explain phenomena that occur with respect to the use of an artefact, its perceived usefulness and its impact on individuals and organisations. Most of behavioural science is focused on instantiations i.e. information systems but it is used also with the evaluation of constructs and methods. In conclusion, even though the DR focus is on technology-based design, its link to behavioural science allows us to cover organisa-

tions, policies and work practices as design artefacts (Hevner, March, Park & Ram 2004).

Perspective of Design Research

Effective design research must provide a clear contribution in the area of the designed artefact. According to Hevner at al. (2004), DR may provide three types of contributions based on the novelty, generality and significance of the designed artefact. One or more of these must be found in a given research project. The first contribution is related to the design artefact itself as it may solve the initial problem. From this perspective the IT continuity maturity model has solved the initial problem of improving the implementation of the continuity management practice. The second contribution is the foundation, i.e. the creative development of a novel construct, model, method or instantiation that extends and improves the existing foundations. The IT continuity maturity model is a method that was a novel approach - as it was a totally new approach in the field of continuity management practice in the target organisation. The third contribution is methodologies, i.e. the creative development and use of evaluation methods and metrics for design research contribution. Finally, Hevner et al. (2004) mention that artefacts must be implementable and contribute to the business environment. The IT continuity maturity model was implemented in the case study organisation and its output improved the level of business continuity from the information system viewpoint.

When one considers these DR definitions, a loose connection between the maturity model development and the premises of DR can be seen. As an example, the IT continuity management maturity model is an outcome of a design process. Even though there seems to be a link between the DR and methods of development, Hevner, March, Park & Ram (2004) clearly state that design is both a process of (a set of activities) and a product (artefact).

Building the artefact for a specific problem may solve the initial problem, but the basic question is how well does it work? The evaluation of the artefact provides feedback information and a better understanding of the problem and improving the quality of the product and design process. Hevner, March, Park & Ram (2004) provide a guideline for design evaluation. According to them, the utility, quality and efficiency of a design artefact must be rigorously demonstrated via well-executed evaluation methods. IT artefacts can be evaluated in terms of functionality, completeness, consistency, accuracy, performance, reliability, usability fit with their organisation and other quality attributes. The core of this thesis is the value evaluation of the IT continuity maturity model. Design Research provides the premise for the maturity model evaluation.

Perspective of Action Research

Action research (AR) is, by definition, active and tightly bound to real life problems in organisations, it may also provide a practical means to reflect theory and practice on a highly pragmatic level. In order to have a working connection to real life problems, the research test subjects are all the actors related to a research problem e.g. developers and tools. This method provides a structured approach for problem solving; finding innovations and solutions for developing organisational capabilities. As action research progresses gradually from problem identification to implementation and thorough testing with the users of a solution, such a relationship may also change the way the community thinks and the way it works, which might affect the research results. For the researcher this means that in practice he must be able to make theoretical interpretations about the new findings and the reasons behind them and, at the same time, be able to contribute to the practical use of the research results (Järvinen & Järvinen 2004, 128 -131).

According to Baskerville and Meyers (2004) there are four premises to consider in order to conduct pragmatic AR. The first is the necessity to establish a theory beforehand for any action. The rationale for this is to avoid actions that are not relevant or valid from the research point of view. The theory behind the IT continuity maturity model innovation originates from learning and improvement models like PDCA model (Moen & Norman 2009) and Six Sigma (Brue 2002). The assumption was that the capability to measure continuity planning and delivery process utility would lead to identifiable improvements in IT continuity management. The second premise is that the problem setting must be pragmatic. In this study, the identification of the most tangible problem related to the IT continuity management led to strict requirements set by the senior management. The third premise requires that the action must inform the theory. According to this, the theory must be validated by its practical outcome. The validation of the IT continuity management maturity model value is at the core of the thesis' objective. The fourth and last premise is related to social situation. This means that the action researcher must be a participant in the action and at same time be an observer. Accordingly there must be collaborative team participation during the action. This ensures that there will be reasoning and social realities while the problem is being solved (Baskerville & Meyers 2004). This implies that actors must trust and be willing to share information with the researcher. This challenge puts the researcher's social and communication skills to test as failure in communication and getting the commitment will probably lead to failure as the research targets will not be as easy to attain (Järvinen & Järvinen 2004, 128 -131).

According to Järvinen & Järvinen (2004, 128 -131), instead of just observing the process and the response, researchers are expected to work closely with the actors and participate in the problem solving. In order to meet this expectation, the researcher has to participate in the actual use of new solutions or at least be present when the theory is put into practice. Close relations with the actual work

may not work for all personalities and may lead to motivational problems. Other challenges are the high expectations of the client or end user. A client may give a lower priority to the theoretical part of the action research as identifiable results matter the most. As a result, the research may turn into a routine and the original scientific research targets may be lost.

According to Davison, Martinsons and Kock (2004), the principle of learning through reflection stems from the multiple responsibilities of the action researcher: to clients and to the research community. This is consistent with the common call for research reports to specify the implications for both practice and (further) research. Clients focus on practical outcomes, while the research community is interested in the discovery of new knowledge. Since the beginning of the IT continuity maturity model development, the collaborative arrangement between the author and the client organisation has been clear, regardless of the author's dual role between the target organisation and the academic field.

From the viewpoint of the target organisation the author's responsibilities included both the key developer and the change agent roles. In the beginning of the maturity model development the author worked as a specialist in the field of IT continuity management. Gradually the initial responsibilities changed from that of specialist to being a member of the senior management at the same pace as the maturity model was being implemented across the organisation's IT. As a result, the role of facilitator of change turned into the overall management of the IT continuity. One could say that the implementation of the maturity model also increased the author's own professional maturity. Throughout the whole process the author was also a member of an academic community, completing an M.A. degree at Laurea University of Applied Science. The dual role as a researcher and the change agent provided an opportunity to share knowledge beyond the boundaries of academics and business.

Evaluation Questions

The IT continuity planning process success criteria have now been in use for three years in Company IT. Continuity management objective settings and status monitoring are based on this maturity model throughout the IT organisation. Although the practice may represent the best practice approach and is linked to industry standards there are still some questions to be asked:

- How well is the model adapted into the organisation's governance model and management?
- Does the approach support the actual implementation of IT continuity planning and has the model increased awareness of continuity management?

- What concrete impacts does this have for service delivery promises and does the maturity model really build assurances that information systems and services can be recovered and restored as required?

To summarise all the questions above; has the Company really gained such tangible benefits that this maturity model can be regarded as a reliable approach for IT continuity management performance measurement and should it be used in the future? Can we verify the theory that the maturity model will work as a catalyst for IT continuity management implementation and the improvement of the actual capability to react and respond to continuity related incidents?

The objective for this analysis is to evaluate the IT continuity maturity model development, implementation and implications in the Company's IT department between 2007 and 2009. The outcome of this study should provide insights into the role of a measurable maturity model's continuity management implementation in an IT organisations' management frame work. The ultimate objective is to verify if the model works as a catalyst for improved IT continuity management.

Evaluation Data

According to Järvinen & Järvinen, the most common methods are interviews, observations, surveys and documentation reviews for collecting information for empirical research. All these methods can be divided into subcategories based on the tools used during the research and the role of the researcher. The relationship between the author and the organisation made it possible to use several methods of data collection, of which the most important data sources for this analysis were reviewing the documents and observing the process and its progress.

According to Järvinen & Järvinen (2004, 154-157), data collection using the observation is based on the notes taken by the researcher. In practical terms this means that the quality of the data is fully dependent on the researcher's own experience and training. Even though the research subject's behaviour may increase uncertainty, the flexibility of this approach allows capturing of events and details that could not be found by other means. According to Järvinen & Järvinen, observation as a data collection method fits well with situations in which the research subjects are social groups and processes. This method allows the researcher to be a part of the research subject e.g. participate in the process implementation or its development. Based on the author's role in the maturity model development and the research subject itself, observation as a data collection model was a obvious choice.

During the IT continuity maturity model evaluation data about the use of the maturity model and its perceived value was collected from the following research subjects by use of discussions and observation:

- 20 IT service teams (10 of these managing critical information systems)
- An IT continuity specialist team
- An IT Service management team
- A senior IT management team
- Corporate and IT assurance related specialists (total: 15 people)

According to Järvinen & Järvinen (2004, 154-157), perhaps the biggest challenge in collecting the data by observation is the researcher. The reason for this is the fact that the researcher's own perception about the research subject will have an effect on the interpretations he will make. Basically there are no controls that prevent the researcher from collecting the wrong data and from making incorrect interpretations. Another challenge is how to observe people so that the researcher's presence will not affect the research subjects' behaviour. In order to mitigate the known issues related to the observation method, the author reviewed relevant document and reports on the IT continuity maturity model.

Järvinen & Järvinen (2004, 156) underline that any documentation that is not designed for the purpose of the research is a secondary data source. Regardless of this statement the available documentation concerning the IT continuity maturity model analysis were mostly statistical reports about the process implementation and recovery capability. So, even though the documentation was not designed for the research, evidence for the maturity model evaluation was available. The following document types were reviewed and analysed by the author;

- documented statistics from information services' quality and trends
- critical incident reports and business impact analysis
- continuity maturity monthly reports
- documents about ongoing continuity development actives
- individual incentive score cards
- IT score cards.

Measuring the Maturity Model

Hevner at al. (2004) provide a guideline for design evaluation. According to them, the utility, quality and efficiency of a design artefact must be rigorously

demonstrated via well-executed evaluation methods. IT continuity management maturity model evaluation is based on both qualitative and quantitative measurements. The qualitative measurement is based on the perceived value of the maturity model for the users and the stakeholders. In practice this is based on how well the IT continuity maturity model serves the users' and the stakeholders' objectives. The analysis is based on the author's observations and impressions of how the users and stakeholders utilise the IT continuity maturity model. In this context users are all individuals, teams and units who utilise the IT continuity maturity model partly or fully in their work and objectives. A stakeholder in this context refers to the people in charge and representatives of governance and management models related to IT continuity management. Based on this, the taxonomy of the organisation entities and subjects represents the users' and the stakeholders' viewpoint;

- service management
- line unit organisations
- IT governance
- corporate governance, and
- individuals.

The quantitative analysis is based on statistics derived from the incident and maturity level reports. The following chapters will introduce the concept of quantitative analysis used while estimating the value of the IT continuity management maturity model for the organisation. Quantitative analysis is based on the;

- documented statistics from information services' quality and trends
- critical incident reports and business impact analysis
- continuity maturity monthly reports.

Tangible outputs from continuity planning are solutions that are not only reactive controls but also increase the level of an information system's resilience. Not all incidents can be avoided, but if the IT environment is designed to be fault tolerant and resilient, incidents should not escalate to a critical level as controls will prevent this from happening. The theory is that there should be a positive correlation between the number of critical incidents and the continuity maturity levels. The basic assumption is that when an IT service has a tested plan of how to respond to different situations they should be able to limit the damage so that the incident will not escalate to a critical level. As a result, the number of critical incidents should decrease as the maturity levels rise.

The total time of service recovery and restoration is dependent on the incident respond time so it is important to keep this time as short as possible. One way to assess the success rate is to collect actualised incidents and evaluate the speed of the incident response. The basic assumption is that there is a positive correlation between the short resolution time and the continuity maturity levels because testing and exercising should improve the response time.

If a critical incident occurs, despite all the preventative actions, timely recovery actions are required. Successful recovery can be analysed by using two units of measurements. Recovery time objective (RTO) is the target time set for the resumption of product, service or activity delivery after a incident. If recovery is successful the recovery time should not be more than that agreed on in the continuity plans and service level agreements. The second unit of measurement is a recovery point objective (RPO), which is a point in time by which data has to be recovered in order to resume IT services. In practice successful recovery is made if the usable data restored is not older than that agreed on in the continuity plans and service level agreements. In order to define what successful recovery is, both RTO and RPO requirements must be fulfilled.

The bottom line from the business point of view is that IT continuity management should be able to reduce the loss of business and the cost of downtime. If the continuity management maturity model creates real value for a business, it must be visible in terms of money saved. The basic assumption is that higher maturity levels correlate with a decreased level in the total cost of a downtime. The total cost of downtime in this case includes the sales value lost, service and product production costs and the cost of the resource (time, money and tools) used during the recovery.

Evaluation of the Maturity Model

ISO/IEC 20000 (2005) standard provides a management system for information services. This model integrates a number of IT processes into one management system allowing the IT organisations to avoid overlapping between the processes, to allocate resources, to measure activities against objectives and to improve process performance.

The overall goal is to meet end customer quality requirements by managing costs with a balanced level of assurance of service continuity. Service management follows the plan, do, check, act methodology, whilst simultaneously managing process to process alignment, change management and linking to the business objectives and requirements. Service continuity is one of the main processes the objective of which is to ensure that agreed service continuity and availability commitments can be met in all circumstances (ISO/IEC 20000, 2005).

The purpose of service management was to provide a central management entity and unify all IT service demand and delivery processes. At that time all relevant IT processes were reviewed against the ISO/IEC 20000 standard before implementation. In order to have successful integration between the processes it was seen as vital that;

- roles and responsibilities were defined in each process
- process terminology and deliverables were equivalent to ISO/ IEC 20000
- the monitoring, measuring and review methods for each process were defined.

The IT continuity planning process was built on five phases. The first phase objective was to understand reasoning, requirements and risks regarding continuity management. This phase required strong competence in business case building and impact analysis as well as direct interaction with business stakeholders. The objective of the second phase was to identify and list available solutions with cost/benefit calculations.

Approval for the final selection was received from the business owner before starting the implementation. As the service managers' role was considered important in requirement management it was natural that responsibility for the first two phases was given to service managers.

The objective of continuity planning phases 3, 4 and 5 was to implement selected solutions, ensure competencies and verify continuity solution functionality by carrying out technical exercises. The implementation of the three phases was assigned to computer managers and technical configuration managers, who were already responsible for service deployment and delivery.

Due to the similarity between the tasks in continuity management the general IT management workloads did not grow. Resulting from this, incorporating the continuity planning responsibilities as part of managers' current roles increased their commitment significantly.

In order to support the implementation of the Responsible, Accountable, Consulted and Informed (RACI) table (table 3) it was published and communicated widely throughout the Company:

		Service manger	Computer manager	Configuration manger	Continuity team	Process owner
Create	Initiate and co-ordinate IT continuity creation process	A/R	C	C	C	I
	Understand risks and business impacts	A/R	C	C	C	I
	Assess solutions and get business approval	A/R	C	C	C	I
Deploy and maintain	Implement the plan according the strategy	A	R	C	C	I
	Communicate the plan scope and objectives	A	R	C	C	I
	Maintain competence by training	A	R	C	C	I
	Test the plan regularly	A	R	C	C	I
	Up-date the plan on demand	A	R	C	C	I
Continuity management	Process and documents validation	I	I	I	R	A
	Monthly management reporting	C	C	C	C	A/R
	Process development	I	I	I	R	A
	Process communication and awareness	I	I	I	R	A

Table 3: IT continuity management “Responsible, Accountable, Consulted, Informed” model (RACI) (Syrjänen, 2009).

According to ISO/ IEC 20000 (2005, 12), an IT service continuity strategy should be based on the maximum acceptable continuous period of lost service and degraded service levels during a period of service recovery. Continuity plans should be extended to take into account dependencies between service and system components. These documents should be stored and maintained so that they are up-dated and available when needed for recovery purposes (ISO/IEC 20000, 2005).

The validation process of the IT continuity documentation verified that the outcomes of each phase were consistent and the document quality met the standards. Having validated the service continuity planning deliverables, the validation team informed the IT service team about the results. This information was also delivered to the IT continuity management process owner, whose responsibility was to provide an IT level continuity status report to senior management, as described in figure 3.

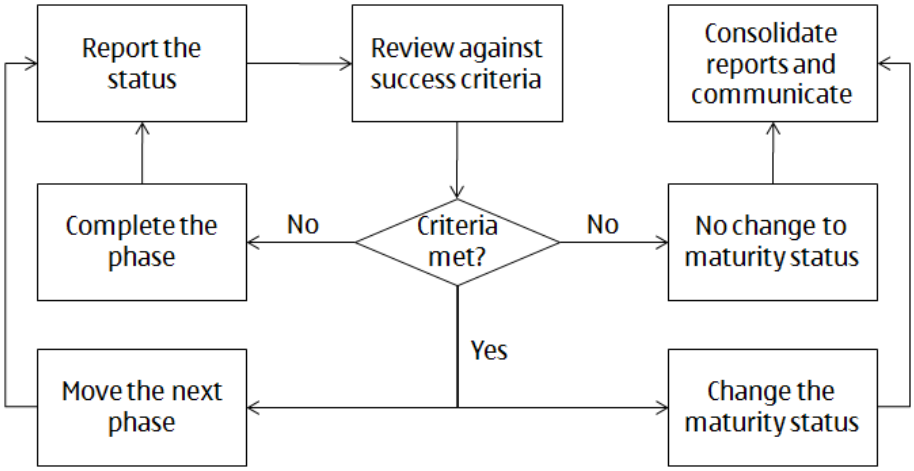


Figure 3: Maturity status validation process (Syrjänen 2009).

However, it was found that the overlapping documents could create confusion among users, and it was thus imperative to review all IT planning and operative documents and align these with IT continuity related documents. For this reason the IT continuity team developed and released document templates for continuity planning purposes. For example, IT backup, recovery and restoration instructions were defined as sub-documents for the purpose of combining all the proactive and reactive controls together. In addition to the IT continuity plan template, risk, impact analysis and technical exercise result templates were released.

In order to ensure that relevant IT continuity documents are created and stored appropriately, IT services must pass a validation before they are allowed to move on to the next phase of the maturity model. This validation was carried out by continuity professionals, who reviewed the content and the result. To make sure that IT services understood the reasoning for approval and rejection, validation criteria have been published and shared with all services. The validation criteria contain a checklist that IT services can use for self-assessment before sending documents to the validation team. The openness with the maturity level evaluation and the use of a common scale for measuring the progress built confidence between the continuity specialist team and the service managers.

After reviewing the process used in IT continuity management, the IT service management developers supported the idea that the process could be integrated directly into the IT service management model without additional changes. This impartial expert review also proved that the model was consistent with industry standards and could therefore be easily used either as an independent management system or as a subsystem of another management system. One of the findings was that the true driver was not the process itself

but the use of simple tools and the division of clear responsibilities between teams and managers.

Value to the Organisation

Company IT is a matrix organisation. On the vertical axis operations were process driven and on the horizontal axis dedicated units were responsible for managing resources and assets. The time allocation of the resources was based on the bi-annual planning process. In practice, business objectives were converted into unit, team and individual level objectives for the upcoming 6 months. After the closure of each planning cycle, managers reviewed how well the objectives were met by using criteria for minimum, target and maximum level performance. A successful performance result would lead to a high payout to teams and individuals, while a poor performance would lead to a smaller reward, if any.

As IT continuity management was one of the key areas for having strong business support, the ability to link planning phases into the objective setting and performance evaluation was seen as important by the management. In order to support the units' planning processes and the service team members' objective settings the continuity team developed an IT continuity objectives scorecard. The scorecard provided the baseline objectives and performance criteria for each maturity level. The IT teams were able to reflect on the current continuity maturity status - the one defined in the scorecard and were also able to set new objectives. The important part of each scorecard implementation was to generalise it in such a manner that the scorecard could be adapted across the IT organisation. This allowed a wider group of IT professionals to be part of the continuity maturity model's objective settings.

Team objectives on the scorecard were initially designed so that IT service teams' achievements were expected to progress level by level until the highest level of maturity was reached. After the highest maturity level was obtained the teams' objective was to focus on different types of continuity exercises. Later, the objective scorecard contained two measurement parts, which focused objectives on the continuity exercises only.

The target groups for the first part were all the IT service teams whose applications' continuity maturity status were at phase 5, meaning that all their phases were completed and validated by the continuity team. For this target group the objective was to maintain a phase 5 status by providing sufficient evidence on how well the technical exercises were conducted and what action plans for improvements were available. The target groups for the second part were the teams whose applications' continuity maturity status was below phase 5. For these teams the objective was to complete the planning and implementation phases including the technical exercises.

In order to achieve the maximum performance level IT teams had to complete the continuity exercise. Integrating the reward system with the maturity model increased the number of technical exercises and the assurance of working recovery solutions. One of the key challenges was the fact that, due to several reasons, the technical exercises often needed to be postponed. This might have decreased motivation and affected the teams' commitment. The challenge was solved by designing the risk acceptance criteria that would be signed by the business owner, thus freezing the IT continuity progress until it could be continued. This approach ensured that even if the IT continuity planning progress was on hold, it would not have a negative impact on the reward system for individual employees.

The overall perception is that the IT continuity management maturity model provided a solid foundation for line management purposes as the planning phases were linked to people's roles. One of the success factors in getting teams and individuals to commit to the continuity objectives were the transparent and equal performance metrics used.

The value to the IT governance

IT governance integrates and institutionalises good practices to ensure that an enterprise's IT supports its business objectives. It enables an enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities and gaining a competitive advantage. IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives (COBIT 2007, 5).

To put it short, a well established IT governance model should ensure that;

- IT enables the business to maximise benefits and opportunities
- IT resources are used responsibly
- IT risks are managed appropriately

According to COBIT (2007), strategic alignment focuses on ensuring the linkage between a business and its IT plans by defining, maintaining and validating the IT value proposition and aligning IT operations with enterprise operations. Due to the nature of the business and end customer expectations and regulations, business continuity management has an important role in the Company's strategic initiatives and operations. For example, business continuity related policies require each business and support unit to implement continuity management practices throughout a whole organisation. With the help of the IT continuity maturity model, the IT directors were able to demonstrate that continuity manage-

ment was aligned with the strategic and operational objectives of the Company. The capability to demonstrate the managed approach has strengthened the business directors' trust in IT's capability to ensure the continuity of the IT services.

Value delivery is about executing the value proposition throughout the delivery cycle. In practice this means that IT delivers the promised benefits against the strategy by concentrating on optimizing costs and proving the intrinsic value of IT. The IT continuity maturity model was designed so that process steps, which would normally be extensively documented, were summarised into few pages and support documents. In addition, the work routines were embedded in the normal management processes to avoid overlaps with similar processes. All the above reduced the complexity of the process and optimised the planning and implementation work.

One of the key objectives for the business critical processes was to decrease unplanned downtimes. After the comparison of the monthly availability reports and the IT continuity maturity levels the correlation between decreased down times and higher maturity levels was undisputed. For example, one of the business owners reported an incident related to a failure in IT: "We faced a serious incident and invoked the continuity plan. Thanks to the exercises we managed to recover and restore the system so fast that there was neither downtime nor slow down" (Major incident report 2009). Due to the continuity management maturity model the Company has gained remarkable savings and increased customer satisfaction. Whether this could have been achieved without the maturity model is not known, but the results displaying the correlation should not be ignored.

Resource management is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure (COBIT 2007). In order to ensure the optimal implementation of the IT continuity management maturity model it was enforced only for the IT systems and services related to critical business processes. For the non-critical IT services the use of the maturity model was optional. As a result, this increased teams' commitment as now there was a rationale for why the IT service team should use time and resources for continuity planning.

The tangible benefit of using the maturity model reporting function was that it provided a transparent information hub between the critical IT services. In practice, IT services could collaborate and plan objectives that would support the resolving of mutual challenges - like reusing a common recovery solutions. As a result IT service teams avoided double work and increased the efficiency of the organisation.

The primary target of the IT continuity maturity model was to steer planning teams step-by-step to continuity planning and implementation. Even though the focus was more on overall process management, the deliverables from each process phase provided information for other management purposes. As the business impact analysis included loss value calculations and information about cross dependencies, the results could be used for information systems classification. Communicating the findings of the continuity tests and exercises improved end-to-end continuity planning between the business and IT units.

According to COBIT (2007), risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding risk management responsibilities into the organisation. From the risk management viewpoint the maturity model and its deliverables provided valuable information for several purposes. Firstly, the phase performance criteria required that each critical IT service must complete a risk analysis in order to progress to the next maturity level. Continuity risk analysis provided insight into risks related to technology, people, processes and infrastructure. All these may interrupt the services for a prolonged time or, even worse, cause a total loss of data. By comparing the results of risk analysis across the IT services and IT units, risks managers were able to identify signs that may indicate changes in the risk level and which would therefore require more attention from the management.

Risk, by its very definition, always includes uncertainty about the severity of an impact and the probability of occurrence. The phase 5 performance criteria of the continuity maturity model required that an application and service should have undergone technical exercises. The technical exercises provided risk management with information about the Company's capabilities to respond to interruption and disruption risks, and thus reveal the residual risks. The ability to measure and provide validated technical exercise reports was valuable for corporation risk management, as this information could be used for group level risk reporting. One of the most concrete benefits was that maturity level information could be used for insurance negotiations. The ability to demonstrate tested and validated continuity plans did have a positive impact on the insurance premiums.

According to COBIT (2007), the purpose of performance measurement is to track and monitor strategy implementation, project completion, resource usage, process performance and service delivery. For example, this can be done by using balanced scorecards that translate strategy into action to achieve goals. The assessment of process capability based on the COBIT maturity models is a key part of IT governance implementation. After critical IT processes and controls have been identified, maturity modelling enables gaps in the capabilities to be identified and demonstrated to management. Action plans can then be developed to bring these processes up to the desired capability target level (COBIT 2007, 5).

With the help of the IT continuity maturity model it was possible to create a scalable scorecard that transformed planning phases into measurable actions. The standard unit for measurement was a single IT system and its maturity level. Table 4 demonstrates how to measure the number of critical IT systems that have met the continuity maturity performance criteria on each of the four IT units (A, B, C and D).

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
IT Unit A (16 IT systems)	3	5	4	2	4
IT Unit B (13 IT systems)	1	4	2	4	2
IT Unit C (16 IT systems)	0	2	4	5	5
IT Unit D (21 IT systems)	5	6	7	1	2
TOTAL:	**9**	**17**	**17**	**12**	**13**

Table 4: The simplified scorecard for maturity measurement. The given values are only examples, not real figures (Syrjänen 2009)

The simplified scorecard provided a snapshot of the current situation of target units and IT systems, but as such did not provide enough information for continuous monitoring and reporting. The gap was solved by combining each system's maturity level with the time dimension. This simple approach made it possible to create an IT continuity maturity scorecard that could be used for reporting the continuity management status of the whole IT. For the purpose of this thesis the author has designed an illustration of the IT continuity maturity scorecard (Attachment 3) with pseudo data.

Status bars on the IT maturity scorecard (attachment figure) show how the imaginary IT teams are progressing with the given continuity planning objectives. As this example demonstrates, the first part of the year shows that most of the measured IT systems were at the initial phase of making business impact analysis and collecting requirements. Based on this information the conclusion is that there is 0% assurance that systems are recoverable in the case of a major incident. Status information from June shows that 25 systems out of 40 have completed the technical exercise required in phase 5 by successfully demonstrating verified capability in recovery and restorations. The remaining 15 cases have progressed well and their continuity capability is not yet proven. When reviewing the year end results, we can make a few observations. There have been changes between the initial number of the measured units and the end year numbers. The most common reason for this is the natural lifecycle of the IT systems e.g. ramp downs and integrations. Approximately, 95% of the systems

managed complete technical exercises, which can be translated as an increased level of assurance in recovery capability. Even though this is merely an example of how to use the IT scorecard, it does underline the importance of consistent and comparable metrics. A useful side benefit is the power of visualisation when communicating the results to the senior management.

The office of CIO (CIOO) was responsible for collecting and consolidating all information about the quality of operations and the progress of strategic initiatives. Along with other priority IT processes IT continuity was one of the key processes that needed to be reported to senior management. A challenge for a small unit was how to be able to keep the reporting process light and still be able to provide reliable information for the IT scorecards. This problem was solved by using the IT continuity maturity model reports.

Due to the simple model, continuity status information was collected directly from the IT service teams and analysed in a relatively easy manner. The status of continuity management was easily adopted by the senior management, as the link between the continuity objectives and performance was consistent and traceable. For the first time senior management could set measurable objectives for the whole IT with regard to continuity planning and be able to follow its progress. Possible issues on the progress were easy to spot and, if necessary, management could initiate corrective actions and allocate extra resources for continuity management.

Value to Corporate Governance

According to the Finnish Central Chamber of Commerce (2003), corporate governance can be defined as a system that helps managing and controlling the enterprise. In order to succeed in this objective, enterprises are expected to comply with several regulations and external drivers. The term compliance is either a state of being in accordance with established guidelines, specifications or legislation or in the process of becoming so. In the legal system, compliance usually refers to behaviour in accordance with legislation. Compliance in a regulatory context is a prevalent business concern; in the Company compliance can be split into two areas 1) compliance against external regulators and 2) compliance against internal regulators.

The information security and crisis management policies of the Company state that information services must provide documented business continuity and disaster recovery plans. This requires rigorous action in order to ensure that business continuity arrangements will work within critical timescales as planned. Corporate IT has responsibility for developing a framework that includes plans and procedures for building resilience on such a level that it will support business in a balanced manner. The given policies underline the importance of the

validation of the agreed action, therefore plans should be reviewed and tested on a regular basis and in case risk levels have increased.

The Sarbanes-Oxley Act (SOX), issued for U.S. legislation by the Securities and Exchange Commission (SEC), requires enterprises to document audit and use controls to ensure the correctness of financial reporting. The common assumption is that continuity management is part of the SOX control frame, however the standard clearly states that a company's business continuity or contingency plans have no effect on its current ability to report financial status. Although continuity management is not a mandatory control, daily backup procedures should be addressed in a management's assessment of internal control over financial reporting. Appropriate backup and recovery procedures allow for proper control over the restoration process and ensure the integrity of the information; therefore it provides an important financial reporting control (Price Waterhouse Coopers 2004, 67).

New York Stock Exchange NYSE Rule 446 (2004) requires that members and member organisations must develop and maintain a written business continuity and contingency plan establishing procedures relating to an emergency or a significant business disruption. In addition, each member or member organisation must disclose to its customers how its business continuity and contingency plan addresses the possibility of a significant business disruption and how the member or member organisation plans to respond to events of varying scope.

Security, internal control and risk management functions' role is to ensure the implementation of the control framework according to relevant regulations and operating principles. As the Company's own policies and the external regulations require it should be able to demonstrate its continuity capability, which also covers information systems. In addition to the need to comply with the regulations and policies, external groups can request information about the current continuity status while securing their own delivery channel and business. For example, insurance companies regularly assess risk levels as a part of an insurance practice and information system related risks are given on this assessment.

Regulations, policies and best practices emphasise that IT continuity management and recovery planning are two of the key controls in minimising the loss of critical data and ensuring continuous business processes. An important success factor for an external audit or assessment is an organisation's capability to provide fact-based information about the effectiveness of its controls and coverage over the company's critical functions and its assets. Due to a consistent and verified maturity model, the Company's IT has the ability to deliver up-to-date fact-based information about the capability of the IT services and systems to respond and recover in case an incident occurs. In addition, the demonstration of rigorous continuity management system builds trust between the Company and its partners and co-operation with the local emergency authorities.

From an internal control, security, and risk management point of view, the maturity model has provided an excellent tool whenever there has been a need to review and report IT continuity capability to stakeholders. In addition, the continuity maturity model has been so effective that it has been benchmarked by other process areas and adjusted for their own use. This may provide an excellent answer to the question “did the model bring any value to business”?

Value to individuals

“What’s in it for me”? This is a question we all would probably want to ask when we start working with new tasks like IT continuity management. For the past three years my position has allowed me to have constant communication with the IT service team members. This communication has contained two main topics: 1) explaining to the new service managers what IT continuity management is all about and why they need to do it 2) discussing and agreeing on a given team member’s individual objectives and incentive planning.

What our continuity management team and I have found out is that the topic continuity management is a difficult subject for many. Resistance to change seemed too high at the start of communication but disappeared soon after. Based on the feedback from the IT managers the workflow was easy to follow as the steps were practical and target oriented. The success criterion of each phase emphasises the end result and allows the person responsible to decide how to accomplish a result. So when I collected feedback about the model, in most of the cases the answer was “I understand what is expected from me and I can choose how to do that”. In my opinion this demonstrates how important it is for the doers to control their own work in order get a high level of commitment to the objectives.

Individual incentive planning is one of the most important reward systems in the Company. From an individual’s point of view it is important that objectives can be set and measured explicitly in order to avoid any interpretations about the level of achievements. Another important feature was that the objectives are fixed, not changed randomly. For both viewpoints the maturity model provided a structured solution as IT continuity management objectives are based on static and measurable success criteria. This transparent approach allowed IT managers and their team members to include continuity management related tasks as a part of the individual reward system.

Conclusion

The overall goal of this thesis was to review what kind of value the IT continuity maturity model has brought to the target organisation and its business objectives. Based on the findings, my perception is that the model has worked as a catalyst for increasing awareness about continuity management.

At the time of writing this, the maturity model has been used for three years and is a widely adopted method of setting objectives and measuring success in continuity planning. The way people communicate continuity capability demonstrates how well the model has been accepted among various interest groups in the IT organisation. It is notable that stakeholder's from business and IT management understand in a consistent manner the reported maturity levels. When communication reaches a level where a single value and its implications are understood widely in the same way, it indicates the successful implementation of a common model and terminology. It is safe to assume that one of the success factors for the implementation was a simplified process model using terminology that is familiar for most of the process-oriented teams instead of using business and IT continuity terminology. This, in turn, made the simplified senior management reporting possible, as senior management understood the content of the report. I believe that this was the key for increased management commitment and support for IT continuity management.

The maturity model was tightly linked to individual objective setting and the reward system, so it is natural to assume that using the maturity model the teams' commitment to the timely planning and implementing of continuity solutions was increased. Recent observations among the IT service units revealed that the IT service teams are interested in using the maturity model as part of their incentive planning. This kind of feedback increases confidence that the model measures the right things at the level of personnel management. Linking the model to the reward system has also increased curiosity among other sections than the critical IT service teams.

Observations revealed that IT services that had reached maturity level 5 managed critical incidents and recovery actions successfully in all reported cases. Even though the number of incidents was not significantly reduced, the number of critical incidents decreased as incidents were handled in a timely manner before they could escalate to a serious level. In terms of money, the correlation between the cost of downtime and the maturity level was obvious: the higher the maturity level, the lower the total cost of downtime. Thus, the IT continuity management maturity model business benefits were realised in a very tangible observable way.

In this study, the success factor for the maturity model implementation was the way it connected IT service teams' incentive planning to the completion of successful technical practise and exercises and gained the senior management's attention. As an indirect consequence of this method the increased management support enabled IT service teams to build solutions that prevent and limit the critical incidents in practice. The inevitable conclusion is that the maturity model (soft approach) had a positive effect on the designing of resilient information systems (hard approach) and increased the assurance of effective IT continuity management. Summa samarium, the maturity model did make a difference as it

pulled the IT organisation into an IT continuity management practice in which no previous method had succeeded.

Discussion

As the scope of this thesis was a large and relatively homogenous organisation, the observations may not apply to other organisations in a similar way. In order to validate the results from this study, one should conduct a similar type of research in another organisation. By extending this research to cover more than one organisation a researcher should be able to do benchmarking between the organisations studied. This may be somewhat challenging as, based on my personal perception and experience in the field of business and IT continuity management, maturity models are rarely used.

Although the research results were surprisingly positive, one question remains: could this achievement have been reached without the IT continuity maturity model? In order to be able to answer this question, the unique element of the maturity model that underlines its success must be identified. In my opinion the key was the means to convert a standard process into pragmatic and measurable steps so that the whole concept was understood by the senior management. In brief; the model succeeded in drawing the management's attention. Regardless of the method, standard or language I strongly believe that any method will succeed if it has management support from the very start of implementation. Thus, this research also reveals the necessary success factors for implementing any type of process. My conclusion is that this achievement could have been reached by other means too as long as management support was secured. I believe that in order to design a working maturity model, an understanding of an organisations' management practices and a dynamic that motivates people, such as individual incentives is required.

When discussing the results, it is sensible to take a few steps back and reflect on the results using an objective method of measurement. This can be done by using a commonly accepted maturity model originally created by P. Crosby in 1979 and later developed and maintained by Carnegie Mellon University and Software Engineering Institute. The Capability Maturity Model integration (CMMI for Services 2009) also known as CMMI is a collection of best practices from government and industry. Over time, the model has evolved and the latest version is targeted at the evaluation of information and IT related process maturity levels reflecting the following industry standards;

- Information Technology Infrastructure Library (ITIL)
- ISO/IEC 20000: Information Technology—Service Management
- Control Objects for Information and related Technology (CobiT)
- Information Technology Services Capability Maturity Model (ITSCMM).

CMMI highlights that the quality of a system or product is highly influenced by the quality of the process used to develop and maintain it. In practice this means that the maturity level of an organisation provides a way to predict its performance in a given discipline or set of disciplines e.g. BS 25999 and BS 25777 continuity standards. According to the standard, experience has shown that organisations do their best when they focus their process improvement efforts on a manageable number of process areas at a time. The standard provides five maturity levels, which are used to characterise organisational improvement relative to a set of process areas, and capability levels to characterise organisational improvement (CMMI for Services 2009).

On maturity Level 1 processes are usually ad hoc and chaotic. The organisation usually does not provide a stable environment to support processes (CMMI for Services, 26). Reflecting this definition, the Company IT continuity management model is far more sophisticated as it is fully managed and organised.

On maturity level 2, projects, processes, work products, and services are managed. Process adherence is periodically evaluated and process performance is shared with senior management (CMMI for Services, 26). Reflecting the maturity level 2 definitions, the IT continuity management evaluation proved that the process is managed as there are nominated people whose responsibility it is to develop and implement the model. As demonstrated earlier, the maturity model is used for management reporting and providing information to senior management on how the IT continuity management implementation is progressing.

On maturity level 3, rules are integrated into the current process portfolio. Processes are well characterised and understood and are described in standards, procedures, tools, and methods. On maturity level 3, processes are described more rigorously than on maturity level 2. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, and verification steps, outputs, and exit criteria (CMMI for Services, 27).

The IT continuity maturity model is defined, documented and provides tools for each process phase. Roles and responsibilities are defined and, furthermore, there are clear verification steps in order to keep the quality of the process outputs on a desired level. In this case the desired level is the capability to respond to incidents and continue operations without interruptions. Evaluation has proven that all the CMMI maturity level 3 requirements are carried out; in some cases in a rigorous way e.g. when it comes to technical exercise requirements.

On maturity level 4, the service providers establish quantitative objectives for quality and process performance and use them as criteria in the managing processes. Quantitative objectives are based on the needs of the customers, end users, organisations, and process implementers. Quality and process performance is understood in statistical terms and is managed throughout the life of the

processes. Performance models are used to set performance objectives for service provider performance and to help achieve business objectives. A critical distinction between maturity levels 3 and 4 is the predictability of process performance. On maturity level 4, the performance of processes is controlled by using statistical and other quantitative techniques and is quantitatively predictable. On maturity level 3, processes are typically only qualitatively predictable (CMMI for Services, 28).

A fundamental part of the IT continuity maturity model is the ability to incorporate process steps into the performance evaluation of people and teams. If there is a known level of performance it is possible to predict the remaining assurance regarding the continuity capability. This information can be used for setting new objectives with delivery time requirements. As demonstrated earlier, the capability of the IT continuity maturity model was linked to the metrics that are used for statistical analysis about the process effectiveness and realised benefits.

On maturity level 5, an organisation continually improves its processes based on a quantitative understanding of the common causes of variation inherent in those processes. A critical distinction between maturity levels 4 and 5 is the type of process variation addressed and accepted by the organisation. In practice processes tend to evolve as other processes and renewed requirements affect the model. (CMMI for Services, 28).

IT continuity maturity model evaluation did not reveal how the continuity management process variation is controlled. However, the study showed that the maturity model itself has had an effect on other IT service processes. While writing this thesis, ITIL 3 implementation had progressed to a stage where all IT service processes are integrated into one manageable entity. That also includes the IT continuity management process. This raises the question and concern of whether ITIL 3 implementation will affect the maturity model. Initially the maturity model was designed so that ITIL 3 was noticed among other standards. Due to the consistency between ITIL 3 and the maturity model it is likely that the change will have a minimum impact on the integrity of the maturity model and its capability to enhance continuity management execution. I am confident that the maturity model will remain intact when it encounters pressure from process development. I believe that the biggest risks are to those individual contributors who will promote change based on their own preferences, even if this conflicts with recognised benefits. It is hard to predict the future, but I feel that as long as the maturity model provides fact-based status information, guides the activities, and has a link to individual level rewarding the integrity of the model will be secured.

Based on a comparison between CMMI maturity levels and the results of the maturity model evaluation results, a few conclusions can be drawn. First of all, CMMI level evaluation would not succeed unless the relevant information was available. The reflection with the recognised industry standard strengthens my

opinion that this thesis managed to focus on the most relevant topics and produce information that can be used for overall maturity evaluation. Second and perhaps a more important observation was the fact that the current IT continuity management status has almost reached CMMI maturity level 5. Maturity evaluation provides an accurate and adequate amount of information to conclude that IT continuity management maturity CMMI level is at least 4. The evaluation does not provide enough information to answer the question of whether the IT continuity management maturity model complies with CMMI maturity level 5. The reason for this might be the fact that there has not yet been any major transformation activity, the result of which could be used for the CMMI level 5 reasoning.

My conclusion based on the results of this maturity model evaluation strongly indicates that the model has reached a high level of maturity. In considering this I do not see any reason to continue the action research and recommend closing the cycle and entering a new area of research.

References

Mahdy G. 2001. Disaster Management in Telecommunication, Broadcasting and Computer Systems. Chichester: John Wileys & Sons.

Graham J. and Kaye D. 2006. A Risk Management Approach to Business Continuity. Connecticut: Rothstein Associates.

Brue G. 2002. Six Sigma for Managers. New York: McGraw-Hill.

Järvinen P. and Järvinen A. 2004. Tutkimustyön Metodeista. Tampere: Opinpajan Kirja.

The IT Governance Institute 2007. Control Objectives for Information and Related Technology. Rolling Meadows: The IT Governance Institute.

British Standard Institute 2006. BS 25999-1 Business Continuity Management: Code of practice.

British Standard Institute 2008. ISO/IEC 21827 Information technology — Security techniques — Systems Security Engineering: Capability Maturity Model.

British Standard Institute 2005. ISO/IEC 20000-1 Information technology — Service management — Part 1: Specification.

British Standard Institute 2007. BS 25999-2 Business Continuity Management: Specification.

British Standard Institute 2008. BS 31100 Risk management: Code of practice.

British Standard Institute 2008. BS 25777 communications technology continuity management: Code of practice.

British Standard Institute 2003. PAS56 Guide to Business Continuity: Publicly Available Specification.

Pirinen R. 2009. Research Framework of Integrative Action. Americas Conference on Information Systems (AMCIS 2009). August 6-9, San Francisco, California, USA.

Hevner, Alan R.; March, Salvatore T.; Park, Jinsoo; and Ram, Sudha. 2004. Design Science in Information Systems Research. MIS Quarterly. Volume. 28 Issue.1.

Baskerville R. and Meyers M. 2004. Special issue on action research in information systems: making is research relevant to practice – foreword. MIS Quartely Volume. 28 Issue.3, 329-335.

Davison R., Martinsons M. and Kock N. 2004. Principles of Canonical Action Research. Information Systems Journal. Volume 14. Issue 1, 65-86.

Jackson O. 2008. The Impact of the 9/11 Terrorist Attacks on the US Economy. Referred 7.11.2009.http://www.journalof911studies.com/volume/2008.

Puolustustaloudellinen suunnittelukunta Helsinki 2002. New Yorkin WTC–terrori-isku ja toiminnan jatkuvuus, opit suomalaisille yrityksille ja julkishallinnolle. Referred 7.11.2009. http://www.huoltovarmuus.fi/documents/3/WTC-julkaisu_5_2002.pdf

Finnish Financial Supervisory Authority 2004. Standard 4.4b Management of operational risk issued 25.5.2004. Referred 7.11.2009. http://www.finanssivalvonta.fi/en/Regulation/Standards/Financial_sector/4_Capital_adequacy_and_risk_management/Documents/4.4b.std1.pdf

National Institute of Standards and Technology Administration U.S Department of Commerce 2002. NIST Special Publication 800-34: Contingency Planning Guide for Information Technology Systems. Referred 7.11.2009. http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

National Bureau of Standards 1981. Federal Information Processing Standards Publication 87 1981; Guidelines for ADP Contingency Planning. Referred 7.11.2009. http://www.niatec.info/pdf

National Fire Protection Association 2007. NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs. Referred 7.11.2009. http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf

The Central Chamber of Commerce of Finland 2003. Corporate Governance Recommendation for Listed Companies. Printed 9.10.2009. http://www.keskuskauppakamari.fi/kkk/julkaisuja/publications/en_GB/corporate_governance/

Moen R., Norman C. 2009. Evolution of the PDCA Cycle. The Asian Network for Quality Congress (ANQ 2009). September 15-19, Tokyo, Japan. Printed 28.11.2009.http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf.

Price Waterhouse Coopers 2004. Sarbanes-Oxley Act: Section 404 Practical Guidance for Management. Printed 6.7.2009. http://globalbestpractices.pwc.com.

New York Stock Exchange 2004. Rule 446 – Business continuity and contingency plans. Printed 11.11.2009. http://www.nyse.com.

Carnegie Mellon University and Software Engineering Institute 2009. CMMI for Services, Version 1.2. Printed 11.11.2009. http://www.sei.cmu.edu/library/abstracts/reports

Company IT 2007. IT Continuity management process: instructions, scorecards, communication kits and standard operation model.

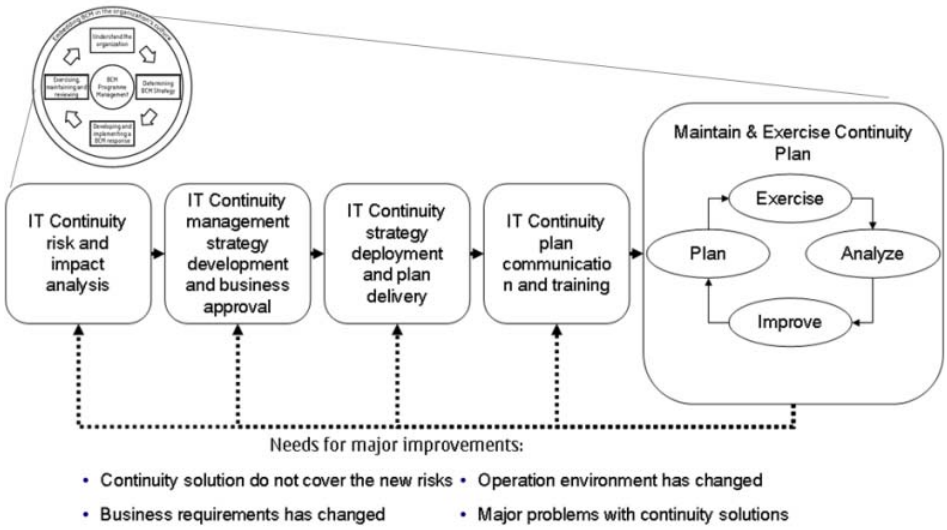
Company 2007. Business and IT Continuity Management Requirements Comparison.

Appendix

Standard name	Standardisation body	Issued
Management of operational risk	Finnish Financial Supervisory Authority	May 2004
31100 Code of practice for risk management	British Standards Institution	October 2008
BS 25999-1 Business Continuity Management Code of practice	British Standards Institution	November 2006
ISO/IEC 21827 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model	ISO (the International *Organisation for Standardisation) and IEC (the In*ternational Electrotechnical Commission)	February 2009
ISO/IEC 20000-Information technology — *Service ma*nagement — *Part 1: Specification*	ISO (the International *Organisation for Standardisation) and IEC (the In*ternational Electrotechnical Commission)	December 2005
BS 25999-2 Business Continuity Management Code of practice	British Standards Institution	November 2006
Federal Information Processing Standards Publication 87- Guidelines for A*DP Conti*ngency Planning	U.S. Department of Commerce, National Bureau of Standards	March 1981
Information and BS 25777 communications tech*nology c*ontinuity management — *Code of practice*	British Standards Institution	November 2008
PAS 56 Guide to Business Continuity Management	Business Continuity Institute, British Standards Institution	March 2003
CMMI for Services	Carnegie Mellon University and Software Engineering Institute	February 2009

Appendix table: A list of industry standards that affect this study (Syrjänen 2009)

The Continuity Planning Process



The continuity planning process as linked to BCM life (Syrjänen 2009)

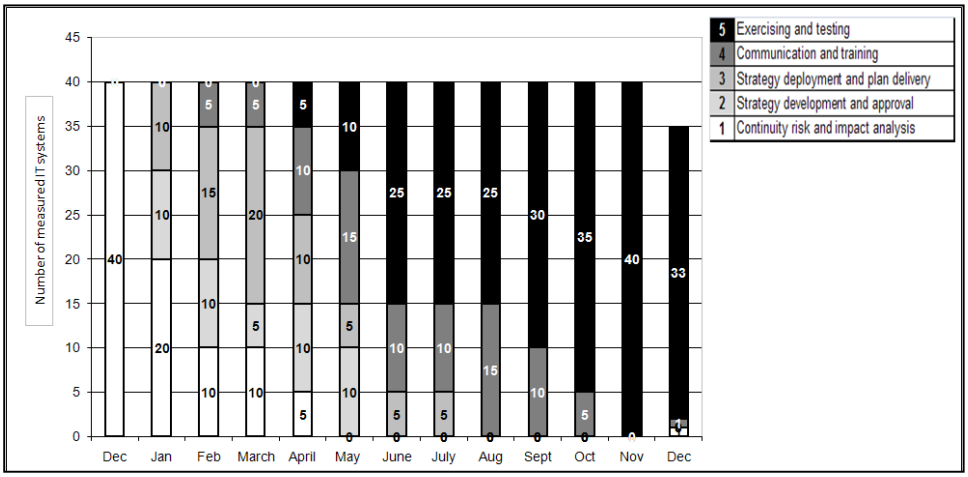
The Maturity Scorecard

RTO= Recovery time objectives and RPO=Recovery point objectives

Reflect current status bellow:	Initial performance criteria			Performance criteria after several observation rounds		
	Min	Target	Max	Min	Target	Max
Phase 0 (new in planning process)	Advance 1 level	Advance 2 levels	Advance 3 levels	Table-top simulation of critical incident invocation and service restoration including a call test of crisis management process, crisis team invocation and communication with business associates		
Phase 1						
Phase 2						
Phase 3			Minimum + demonstrated participation to joint exercise			
Phase 4	Demonstrated table top exercise	Minimum + demonstrated participation to joint exercise	Target + demonstrated technical recovery exercise			
Phase 5				Documented exercise results showing evidence of recovery capability within RTO and RPO	Minimum + follow-up activities to any findings on improvement needs	Exercising of continuity plans including testing of system and data recovery within RTO and RPO, including 1 generation of dependencies OR Verified successful plan invocation and recovery on real incident within RTO

Objectives scorecard comparing initial performance metrics to mature level organization (Syrjänen 2009)

Implementation Example of Maturity Scorecard



The Continuity Maturity scorecard example (Syrjänen 2009)

Chapter 9
Security Management Co-operation with Authorities and Local Community Operatives

The Management of Common Security

Sami Rusanen

Master's Thesis, Laurea University of Applied Sciences, 2009.

The aim of this study was to explore how security is managed in certain multiple tenant state administration premises and housing organisations representing different fields of state administration. On the basis of the achieved knowledge, a model for the management of common security was created. The security management in multiple tenant premises was reviewed in a case study from the point of view of the main organisational actors in the building studied for the research project.

The theoretical part of the study combined the theoretical basis of performance guidance, which is used as the governmental guidance model, and the organisational security management; thus forming an entity with descriptions of the means of achieving its security management objectives. In the empirical part of the study data were gathered from the official documents guiding the security of the multiple tenant premises and by thematic interviews.

The gained information was analysed with the help of theoretical content analysis and guided comparison. The means of achieving the security management objectives were first compared to security management carried out in each organisation, which provided a common basis for measuring the organisations. After that a comparison of results of the organisational actors was made, which facilitated the understanding of the state of the management of common security in multiple tenant premises. The evaluation chart developed within the study is meant to be used in similar studies or reports.

In the security management of the multiple tenant premises several areas for development were found both in the organisations and between them. The reasons for that were mostly due to the lack of a comprehensive security management strategy. The security management of the authorities located in the same building was carried out almost entirely according to the administration's specific requirements. Between the actors, no co-operation was carried out in practice with reference to security management and no agreements were made on common procedures.

Methodical, comprehensive and well-functioning security management would require the forming of a comprehensive picture of security risks in the multiple tenant premises by the actors, as well as guidelines and plans for further developments that should be made on that basis. It is argued that security management should be reviewed through the management of common security for all the actors in the same premises, which in turn would necessitate close cooperation between the actors as well as common principles of action and practices. A particularly important issue is the organisation of common security exercises and training as well as the preparation of harmonised guidelines for different incidents and emergency situations.

Security management carried out in cooperation would increase the synergy between different administrations and improve cost effectiveness by reducing overlapping. Cooperation would particularly reinforce the possibilities of different actors to prepare themselves for common security risks.

Chapter 10
Border Security

A Facial Recognition System as a Maritime Security Tool

Jyri Rajamäki, Tuomas Turunen, Aki Harju, Miia Heikkilä, Maarit Hilakivi & Sami Rusanen

Proceedings of the 8th WSEAS International Conference on Signal Processing Istanbul, Turkey, May 30 - June 1, 2009, ISSN: 1790-5117, ISBN: 978-960-474-086-4.

Extended abstract: Administrating and processing information has been developing fast in the past decades. The human face as a digital image is much easier to produce and to treat compared to our ability to do so in the last century. Digital cameras have replaced traditional photographic methods. The internet is expanding continuously, giving more possibilities to produce and to transmit information.

With the Schengen agreement the inner border inspections were closed down; e.g. the Finnish Border Guard no longer observed and controlled the traffic at the harbours of Helsinki. Freedom of movement has brought new challenges both to the authorities and privately owned companies (shipping companies, expeditors, passenger and cargo transportation etc) in the harbour environment. Without regular border inspections criminals and stolen goods are more easily moved from one country to another. It is likely that the level of active monitoring of the public peace and security has decreased and that alternative monitoring

and control methods are needed. To keep a harbour safe is not just a local issue - it is also important at national and international levels. Today, the government of Finland has a productivity plan which means cutting down man power from the police, the border guard and other governmental agencies. However, as we become more and more international new issues need to be taken care of and new challenges arise as to how to maintain our security. Hence, new kinds of investments are needed in order to maintain security. The facial recognition system (FRS) could be one solution.

This study maps the relevant expertise on the scientific and technical issues related to facial recognition. Experiences are collected from the FRS currently interpretation. When studying these facts the research provides possibilities for adapting and implementing FRS in a real environment. If and when a reliable and cost-effective FRS can be build, it could lead the way to launch the system as a common security tool in harbours.

Face Recognition as an Airport and Seaport Security Tool

Jyri Rajamäki, Tuomas Turunen, Aki Harju, Miia Heikkilä, Maarit Hilakivi, Sami Rusanen

WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, Issue 7, Volume 6, July 2009.

Abstract: The transportation industries have been subjected to unprecedented scrutiny and regulatory mandates in the post 9/11 era. On the other hand, the inner border inspections were closed down in Europe with the Schengen agreement. Freedom of movement has brought new challenges to authorities and transportation companies. Effective camera surveillance with a facial recognition system (FRS) could be a realistic solution. FRS requires camera(s) and a control device; a computer with special software. The software processes the material, e.g. facial images, collected by the cameras. FRS has been used as a monitoring and controlling tool for major events and border crossings. The aim of FRS is to maintain and improve safety and security in a cost efficient way by saving manpower. However, FRS is an additional security tool and therefore not to be trusted on its own. FRS is being used mainly as a verification method where the human face functions to provide access or as pin code. The optimal operational environment for FRS is a dry environment with stable illumination; most likely an indoor environment is needed to guarantee the operational ability. Images of faces should be viewed from a close distance and the persons, who are to be identified, should cooperate. FRS is composition of technical elements and applications which are commonly used in everyday life. FRS can be used when

profiling the environment and setting reasonable aims and in various places. Hence FRS is challenging traditional methods as a sophisticated security tool for the sophisticated situations. So far, the only operational FRS in Finland started in summer 2008 at Helsinki-Vantaa airport. This paper has examined and collected experiences from the airport pilot project, from the relevant literature and by interviewing experts in the security and facial recognition field. The aim of the paper is to specify the desired goal; how can FRS be applied as a new seaport and maritime security tool.

The International and Transorganisational Information Flow of Tracking Data

Jouni Viitanen, Markus Happonen, Pasi Patama, Jyri Rajamäki

WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP '09) Puerto De La Cruz, Tenerife, Canary Islands, Spain December 14-16, 2009, ISSN: 1790-5117, ISBN: 978-960-474-143-4

Extended abstract: In the past decade, tracking has become an essential and valuable tool for authorities to prevent and investigate crimes. At the same time, criminals and organised crime have internationalised - mostly due to European integration. Within the last decade, criminals have also become more technically orientated. Some counter measures for tracking applications have been found in the hands of the criminals, and therefore international cooperation between officials has become even more vital. The change has been rapid and therefore law enforcement authorities (LEA) have failed to create protocols and procedures to deal with international tracking issues.

It is more efficient to prevent than to repair damage. Unfortunately, prevention is even more difficult than crisis management, due to information and time criticality. Currently, the Geographical Information System (GIS) is mostly used for analyzing situations after they have happened or trying to make logistics more efficient, but not for preventing unwanted events from happening.

This paper addresses the problems of LEA with regard to cross-border operations and explains how they differ from other operations. It focuses on the operational level of action and addresses issues across the range of LEA operations. Its goal is to reveal the need for technical help and guidance focused on tasks at borders or co-operation over borders. It examines the special considerations required when conducting operations regarding the complex modern border environment. Many of these problems are also present in non-national or state borders.

Chapter 11
The Critical Mobile ICT Systems of Law Enforcement Authorities and Rescue Services

Designing Emergency Vehicle ICT Integration Solutions

Jyri Rajamäki, Timo Villemson

In Proceedings of the 3rd International Conference on Communications and Information Technology (CIT'09) Vouliagmeni, Athens, Greece December 29-31, 2009, ISSN: 1790-5109, ISBN: 978-960-474-146-5.

Abstract: E.g. Finnish police cars have about 40 different user interfaces (radio, navigation, command and control systems, radar, alarm lights, etc) in addition to a car's standard user interfaces. In cold weather conditions, not all police vehicles create enough electricity for such intensive operations. Also, the wiring and ergonomics are problematic. The annual delivery amount of emergency vehicles is, however, so low that traditional business models, where devices and systems are sold to the end-user, do not motivate suppliers to invest significantly in system development. Therefore, other business models, such as digital service concepts, are needed for security services. In this paper, the concept vehicle discussed is the Volkswagen Transporter used by the Finnish police but the possibility of extending this concept to other emergency vehicles is also presented. A new mobile platform for police cars is proposed, and the digital service design parameters of the potential ICT integration solution are defined. Further research subjects are also presented.

Creating a Service Oriented Architectural Model for Emergency Vehicles

Jyri Rajamäki and Timo Villemson

INTERNATIONAL JOURNAL OF COMMUNICATIONS Issue 2, Volume 3, 2009.

Extended abstract: Emergency vehicles used by police, customs, frontier guards, as well as fire and rescue services are increasingly dependent on ICT systems, especially wireless and mobile communications. In the past decade, an increasing number of new technical devices and systems have been installed in these vehicles, and it is necessary to ensure that information and "on-demand"

services provided by these technologies are delivered reliably and securely through one or more of the recently developed wireless architectures.

There are, however, serious challenges to overcome. As the number of ICT systems has increased, the number of user interfaces of emergency vehicles has increased considerably. This has resulted in functionality problems; for example, the space for airbags to function has decreased. Also, technical problems with regard to electric supply and cabling arrangements have occurred. In addition, the documentation of applied solutions is not always adequate. Another issue is that the longed for standardisation in the field has not taken place. This may be due to the large variety of equipment suppliers or because the annual delivery amount of emergency vehicles is so low that the standardisation has not been given priority by experts in the field. The challenge is to use infrastructure-based communications and ad hoc networks to provide on-demand services in a highly-volatile, complex environment. Thus there is a need to study the smooth interoperability of architectures with regard to emergency vehicles.

This paper (1) illustrates the operating environment: communication networks of public authorities, emergency vehicles, as well as the ongoing change towards service business; (2) describes the main ICT systems of an emergency vehicle with an emphasis on the police car; (3) presents the research method applied in this study: the digital design service approach; (4) presents the findings of this study: a new mobile platform for a police car is proposed, as well as the digital services and the design parameters of the ICT integration solution; (5) outlines a new service model that could be outsourced to 3rd party vendors and the methods that could be used to refine these models; and (6) presents the needs for further research and conclusions.

Information Security in Satellite Tracking Systems

Pasi Kamppi, Jyri Rajamäki, Robert Guinness

In Proceedings of the 3rd International Conference on Communications and Information Technology (CIT'09) Vouliagmeni, Athens, Greece December 29-31, 2009, ISSN: 1790-5109, ISBN: 978-960-474-146-5

Abstract: Satellite tracking is one of the most rapidly growing business areas in the world, and there are already many commercial applications available. Benefits for the customer are advertised, but there is no mention of the information security. Modern satellite tracking systems contain communication on many levels, so they are vulnerable to many risks of information security. This paper covers the main satellite tracking system information security vulnerabilities and gives guidelines on how to make systems more secure.

PART III
Security of Critical Events

Part III includes four chapters. Three of them deal with security of large public events and political meetings; one addresses crisis situations.

Chapter 12 deals with communication and security management co-operation at large events by examining the IAAF World Championships, 2005 in Helsinki. Chapter 13 researches the usability of TETRA networks in a large multi-organisational event. The target event was The Organisation for Security and Co-operation in Europe (OSCE) meeting in Helsinki, December 4-5, 2008.

Chapter 14 includes three studies covering the nuclear security of public events and political meetings. Mobile measurements are needed to search for nuclear material. Traditionally, GPS is used for positioning outdoors as positioning indoors is difficult. In the first study, Syrjälä demonstrates that it is possible to track radioactive sources by utilizing indoor positioning systems based on the wireless local area network. In the second study, Garlacz created a Java application, IPARM, in cooperation with the Finnish Radiation and Nuclear Safety Authority (STUK), with the aim of reducing or removing human error from the accurate positioning of measurement equipment within buildings. The third study carried out by Ilander, Toivonen, Meriheinä and Garlacz, e.g. reveals what encouraging experiences of the field tests were.

Chapter 15 discusses school shootings and other crisis situations as well as the transparent authority of power in law enforcement. In the first study, Sund develops a model of the behavioural threat assessment and management process for educational institutions in the Finnish educational system; in other words it aims to recognise access and manage risks concerning the occurrence of severe violent behaviour in school-like environments. The second study carried out by Ojasalo, Turunen and Sihvonen, is a case study in the context of school shootings. In the third study, Turunen researches the acquisition and dissemination of facts, role shifting and managing the related risks from the perspective of different operations in the public safety field as well as from the perspective of a field actor with the writer's personal experience and experience from the interviewed professionals within this context. The fourth study carried out by Viitanen, Patama, Knuuttila, Rajamäki and Ruoslahti, balances LEAs' video surveillance, audio surveillance and technical tracking rights against the privacy of citizens. The study also outlines a scenario of how common ground can be found with a constructive approach facilitated by advanced technology.

Chapter 12
Communication and Security Management Co-operation in Large Events - Case: IAAF World Championships 2005 in Helsinki

Juho Reivo, Jari Vuoripuro and Nina Pelkonen

Abstract

Inter-organisational co-operation and co-operation between authorities is usually planned but co-operation with private sector security actors has been mostly forgotten. Yet, it is the private security that is commonly the first responder in incidents and responsible for most event security.

Large events can be identified as creating the need for a separate security and safety organisation and preparedness planning where several security actors are involved. Here communication is critical but systems in events are set up more ad hoc than normal. A communication and management system that is created on top of any technology has to be planned well and take the human element into account or usability is lost. TETRA based equipment is up to the task but it may not be used efficiently. Omissions in regulations also hinder homogenous co-operation across the whole security and safety field.

As the presented research and case study show there are five themes that should be noted in co-operation between organisations. The themes were identified from interviews with management level operational security staff and are; trust, attitudes, knowhow, planning and underlying modus operandi.

To tackle the increasing security needs of large events, public authorities and private security actors have to integrate in better ways in order to manage safety.

Introduction

Security and safety services are in most cases listed as the critical infrastructure of any society. Security and safety include many actors, both public and private. In today's world, the role of the different private security actors is increasing as governments can't provide all the required security alone. In particular, large events require additional resources. In Finland there is practical experience in planned co-operation between all security actors. This paper analy-

ses criticalities in communication and security management co-operation success at the IAAF World Championships in 2005, in Helsinki, Finland.

The IAAF Championships as an event is relatively large and takes the resources of Finland as a venue comfortably close to their limits so that every organisation has to be utilised in some capacity. These levels of time (duration), area (size), participants (amount) and security staff (amount), among others, visibly reveal the challenges and problems there may be when managing such a complex challenge as these organised large events pose.

In fire and rescue services as well as police organisations, command centres and the preplanning of activities is standard but does the private sector security actor fit into those plans? How can all security and safety be better integrated into co-operative security and safety management? These were the questions that we came up as we approached our topic.

Working co-operation and integrated activities are not as simple nor straight forward in actuality. As one of our conclusions is, it is not the technology that prevents the most effective co-operation, it is the human element. This research should build one bridge between the gap that separates technical design from critical communication and the actual manifestation of how it is used in a complex situation.

We will first present some key definitions of this research and its concepts. After a brief background review of the case event, the analysis of the interviews will be presented. We will then reflect on the discovered themes in the three sections centred on management, regulation and organisational culture. Our final section will include suggestions to improve the observed situation as well as concluding remarks.

Definitions of this Research

The topic of this research revolves around event security management and communications and co-operation between organisations. The principal thought driving this work has been to discover what underlying aspects affected the differences within the overall security organisation and between three security command and communication centres that were part of the security and safety management structure of our selected case, the IAAF World Championships in Helsinki, Finland in 2005.

The framework for this research is to look at both co-operation between police, fire rescue and private security. According to Finnish law, the organiser of the event is principally responsible for its security and safety but, as is expected in an event of this size and importance, the roles of governmental agencies and

authorities are very central and directly linked to all security and safety activities. This creates a combination of security actors where in practice the aforementioned three play the most important parts and others – military, customs, Red Cross first aid, volunteers, etc. - act in more supportive roles.

One of the most important parts of complex organisations is communication. In this case it was supported by having most of the security organisation use TETRA-based radio communication as their main communication line. This and other known experiences by the authors of the event led to the communications approach in our research. Our main question is: how can all security and safety actors can be better integrated into co-operative security and safety management? In this, we focused on operational activities in our case study.

Research Methods

The decision was made that themed interviews (Juholin 2006, 355) with the representatives of the main security and safety organisations were the most suitable approach. Research was limited on the management level and the three areas had centralised security and safety commands. Neither physical layouts nor the roles of the people nor the number of the staff were identical. Therefore they were simplified – treated as being equal – for this research.

Interviews were conducted between May 2008 and September 2008. They were done mostly with two sets of questions - preliminary and more topics specific. Some answers were gathered by email and some in face to face interviews. The research team then analysed the answers, identified commonalities, discussed them and proceeded to reflect on them from each member's area of expertise.

Central Terms and Definitions

1) Attitude and Attitude Transference: In this case example, attitude(s) became central in understanding some of the answers from our interviews. Attitudes are based on accustomed practices and traditions, for example whether or not co-operation is a new thing or already experienced. Attitude may manifest as individual like or dislike or organisational attitude where likes and dislikes are learnt from peers and superiors. (Shockley-Zalabak 2006, 55, 140-141).

2) Event Size and Preparedness for It: Events of a big enough scale require a special approach. Large events by definition, we believe, need to be handled as separate entities outside regular daily security management. They often (directly or indirectly) monopolise almost all other activities within their vicinity in a way that it is not possible to include required security measures within daily routines.

No one has made a clear distinction when an event stands out as a "major special event". Some signs are that there is a very large crowd – possibly in relation to the local population. The size and classification of the controlled area; nature and type of the event; VIPs and combination of these and other circumstances ("(inter)national importance" for example) may warrant the special management of security and safety, a joint operation, a (security) project organisation (Turner 1999,124), even though a big event may not be defined by big risks.

3) *Communications and a Communication plan*: Communications means broadly all exchange of information in any form, be it text, radio message, touch, “body language”, signs or even organisational actions. It is plural and includes all activities – verbal and non-verbal as well as intended and unintended. Communication is a complex activity or process in which the effects are hard to predict (Juholin 2006, 16).

The communication plan is the instructions in which it is specified as to who communicates with whom and who may have specific details on what and how something is to be communicated and by what method. With reference to radio communications it specifies for example the equipment used, talk groups (“channels”) and call signs. With TETRA, it must be noted that for all talk groups prioritizing and handset management could be done over the air, which makes it possible to more flexibly change to several possible alternatives - if so planned and trained (Keikkonen, Pesonen & Saaristo 2004, 30-40).

4) *Culture of Activities and Organisation*: Culture in a broad sense includes all human activity and its products. Our research is very much a study on certain activities of security and safety management culture: “Is knowledge sharing encouraged and facilitated?”, “Is there an atmosphere of openness and trust” etc. [6]. In this case we are talking about culture defined more in terms of organisational culture: a complex system of shared traditions, signs, assumptions and other activities that affect how we behave in a given organisational context. Cultural affects and cultural differences should not however be over emphasised. Even when comparing police, rescue services and private security, in most cases (especially in small setting on a national level) we have much more in common than we may think at first (Pinnington 2004, 209-210; Shockley-Zalabak 2006, 47-48, 55).

5) *Safety and Security Actors(s):* Actors are here considered the organisations involved in making the event, acting in a way that supports it. Specifically we discuss the security and safety actors. Depending on context, this may apply to all security and safety organisations or in some cases an actor may refer to only private security personnel as opposed to public authorities, such as police and fire rescue.

For translation purposes, it has to be mentioned that security officer includes both security guard (fi: vartija) and steward (fi: järjestyksenvalvoja) which have a separate legal status in Finland. Safety and security are understood as separate in English but translated with one word in Finnish and thus security is here understood to include safety if not otherwise explained in the text.

6) *TETRA and VIRVE*: VIRVE is a secure communications system network that is used in Finland. It is based on the TETRA (TErrestial Trunked RAdio) standard that European Telecommunications Standards Institute (ETSI) has acknowledged as the only official radio technology meant to be used by public authorities. VIRVE is used by all Finnish authorities nationally, including fire and rescue services, police, border guards, health and social services, customs agency and to some extent the military. Around the metropolitan Helsinki area there is also HELE-NET, which is a TETRA network based system used by an electricity company. VIRVE and TETRA are emphasised as TETRA-based radio equipment was used extensively and played a major role in the organisational behaviour studied (Pursiainen, Lindblom & Francke 2007, 102-110).

IAAF World Championships Helsinki 2005 Background

The 10th IAAF World Championships in Athletics was the largest public event ever held in Finland as well as the most important sporting event in 2005. More than 3,000 participants from over 100 countries, 4,000 media representatives, as well as some 5,000 volunteers helping the organisers and the athletes took part in the event (Hänninen 2005).

The actual World Championships lasted for 10 days. However, the security arrangements were fully functional for two weeks. The security planning had begun as early as two years before the games.

Distribution of Work and Duties

Under Finnish law, the organiser of the event had the primary responsibility of maintaining order and security. To perform this, the organiser employed a private security company, which, in turn, used subcontractors.

During the games, the police had a staff of approximately 1,200 persons at its disposal, rescue services totalled approximately 500 (staff at Helsinki and Espoo, including normal readiness), private security totalled approximately 1,200 in security and hundreds of others were involved as first aid medicals, accreditation officers and in other positions.

Security measures to be undertaken by the organiser under the Assembly Act included providing a necessary number of security guards to maintain order. The

sphere of authority of the organiser included the compound area of the Athletes' Village as well as the immediate surroundings at the various exit gates of the village and the compound area of the Olympic Stadium. The organiser was also responsible for the entry screening of persons and their personal belongings.

The police, who were the main authority, had assistance from other authorities such as the Rescue Department, the Finnish Defence Forces, the Finnish Customs and the Border Guard as well as from private organisations such as the Finnish Red Cross. For this purpose, the police requested executive assistance from other authorities, who then acted under the command of the police authority. In addition to this, the police supervised the organisers in the fulfilment of their duties defined in the Assembly Act.

When necessary, the police took operational command and assumed overall responsibility for performing the security duties by issuing orders to security guards and deploying units inside the Athletes' Village.

When outlining the role of each authority, certain rules were to be considered. It was agreed that the ultimate command authority rested with that authority under whose statutory duty it was to carry out the assignment at hand.

Structures of People and Resources

There were three main operational security command centres. The main command centre was situated at Pasila Police Station. The other command centres were in the Olympic Stadium and at the Police College in Espoo, which was one kilometre from the Athletes' Village. Even though the organisation structures in all of them were similar, there were some differences with the view to the role of the management of the private security. In Helsinki, the management of the private security company took part in the operational command centre, whereas in Espoo it did not. In Espoo the private security had a centre inside the compound where there were representatives from the military (that were under the command of police) and also some informal co-operation with police task groups operating next door.

For communication security actors used VIRVE and other TETRA networks, secure data networks, email, mobile phones and most importantly regular and casual face-to-face meetings to either officially or unofficially convey information and manage event tasks. Different authoritative organisations had some shared VIRVE call-groups but private security actors especially operated with their own radios having only direct connection to operational command centres through their area managers. The centres had at least one handset for listening in to all security related networks.

The Risk Analysis and the Outcome

According to the risk assessment, no serious security threats hung over the games and it was likely that the games would run safely. The potential risks included incidents, traffic jams and accidents. The main objective of the security arrangements was to create a secure and trouble free games in a safe environment.

The analysis of the threats was found to have been a success after the games. The only disturbances during the games were some thefts of TV-sets in the Athletes' Village, occasional "snags" at the security checks, traffic jams, power cuts due to storms and harsh weather, some harassment cases and the removal of an old wartime anti-aircraft grenade from the construction site in the vicinity of the Athletes Village - all in all fairly uneventful for an event of this size.

Interviews with Operational Security and Safety Management Staff

The themed interviews took place between May and September 2008. Most of the interviewees were asked background questions first and a second set of more specific questions later but the first part was skipped when information was available. The answers by and large emphasised the social (human) aspects of the security and safety, communications and management. To emphasise impartiality, it must be stated that none of the generalisations or examples made were based on single answers or one faction's views. Common sentiment on the most interviewed supported all conclusions, although not all expressed any opinion on some points. A definite fault in this research must be identified in the unevenness of interviews as some were conducted via a combination of phone and email and some, at length, face to face.

The Background and Identification of those Interviewed

The interviewees chosen from the police organisation for the interviews were senior officers in charge of the security arrangements in the World Championships 2005, and officers in charge of field and overall operations in the command centres. There were four interviewees; two of them worked in Espoo and two in Helsinki during the games.

From private security the highest ranking members of the management, each working at one of the areas were selected for interviews. All three are veterans with decades of experience in handling event security in demanding high profile settings and they also had extensive experience of working with authorities.

Helsinki rescue services fire chief was also interviewed and he acts as an authority and liaison to the event organisers and to other authorities in regard to events in the Helsinki area. In Helsinki in 2005 he acted as a general coordinator without a specific operational area of responsibility.

The medical organisation selected for their interview a person who works for the Finnish Red Cross's first aid organisation's management and is responsible for the Olympic Stadium area.

Answers – Viewpoints on the Topic

The answers from the interviewees reflect the details they observed that are linked to our presented topic and the sometimes rather specific view of the whole event they had during the games.

All the security and safety related actors had some general notion about and aim towards total security at all levels. One could argue that there was a common goal but the aims were formed separately. All security actors also embraced, on some level, the ideas of shared operational command centres; TETRA based communication, secure and backed up communications and co-operation with all the other security actors. These were their wishes and will – even if the execution was not always smooth.

Besides the common aim five central themes emerged from the analysis of the interviews; trust, attitudes, knowhow, planning and underlying modus operandi. Each theme touched on several issues but these were noticed only in the breakdowns. Also it must be noted that only those themes that evoked memories of problems (own or others) and issues that were seen relevant and worth mentioning in the interviews are presented here.

1) *Trust*: A very central issue in security is trust. Organisations did not trust each other enough to mix and integrate fully but instead worked "alongside" or "at arm's length". Organisational distrust manifested in "officiality": sticking to formal interaction and strict organisational division. The main concerns mentioned for this were confidentiality and information security. The latter was particularly mentioned as a reason for using separate communication networks and equipment instead of a joint channel for general command.

When trust manifested, it stemmed strongest from individual level connections. Individuals from opposite organisations knew each other from previous occasions, although they were not personal friends. However, it took only the few key people to know each other for it to spread by example to all who were working in those particular groups, thus affecting how that local organisation acted in reality. When there was familiarity with the other (person or organisation) there was

no need to prove one's worth and abilities. However, often an organisation was, in some circumstances, excluded or not taken seriously or not listened to.

2) *Attitudes*: Attitudes towards co-operation and other organisations played a significant role. Again, these manifested at both individual and organisational levels, some apparently as faint notions all the time and some sporadically and stronger. Specific attitudes mentioned were around views on roles each organisation had (or should have had). There were signs of not knowing or being able to decide who was or should be in charge at times, if no clear imperative was present. There was an attitude of trying to take over and adopt a position over others – "to be the boss" manifested by "telling, not discussing". This caused friction between all organisations. This was also tied to "blindness" – a denigrating of the roles of others.

3) *Knowhow*: The biggest difference between authorities from different areas and between authorities and private security actors was mentioned as the theme of "knowhow": knowledge and wisdom about what the events are and how to work in them in general and with reference to security. In the interviewees organisations there were also seen to be differences in levels of event knowhow. The authorities were seen by all as having a superior basic level of general security training and experience but the private security possessed more event related specialist knowledge and experience. The requirement to be flexible, which was mentioned as an example, was not understood by those who had not worked closely with events before. By and large, joint exercises had been omitted and would have been wanted, according to the results of the interviews, as tools for both better organisational integration as well as basic special training.

4) *Planning*: Planning was considered to be neither lacking nor particularly overextensive. Te answers reveal some problems. Some practicalities and operational procedures were not thought of, which especially manifested in gaps in the communication plan that had not been taken into account on how two side-by-side organisations (private and public authorities) could or should communicate and on what issues. No plan was known to the interviewed on how security communication would have been handled had all organisations needed to be utilised in an emergency incident. The framework and interface of actual co-operation and its level was apparently worked out at the operation sites. Where possible, old acquaintances "reused" their previous understanding of working together and recycled that familiar way of working into their organisational reality.

5) *Underlying Modus Operandi*: Two operational mode pairs were also discovered amidst the answers. Where problems were seen there was a strong presence of juxtaposing hard ("inflexible", "security overrides customer needs") and soft ("flexibility", "event needs before security procedures") approaches to security. Similarly, the "daily activities" and "preparedness to crisis" were juxtaposed, where in the former the focus was on handling the small more numerous prob-

lems and participant service, while in the latter the focus was more on the less likely larger catastrophes and reserving resources for those. For example, in Espoo, the police had an excellent operational command centre that was ready for catastrophes but was too far away and not ready to handle the more common daily activities that were taken care of at and within the gates of the athletes' village where another command centre was set up, mostly by private security.

Technology Assisting Management

The Rescue Services College's Command Manual (Kaukonen 2005) sums up the basic principles of the management in a rescue operation as requiring real time information, careful planning and long term anticipation as well as easy transference from small to large organisational structure depending on the need. They also apply to the security management of a large event.

Management Responsibility

In the so-called basic state of a public event, where everything is as it should, overall command rests usually with the security management. However, if the situation becomes threatening or in an incident occurs, the overall responsibility is transferred to the appropriate public authority. Managing a hectic emergency situation should run as smoothly as managing a normal, small-scale situation. This means that management organisation is planned to suit all regardless of the agency. A coherent joint operation has the best potential for scaling up to meet any emergency.

The Communication Equipment

The primary users of the Finnish Authorities' Telecommunications' Network, VIRVE, are the various public authorities. However, other users may be allowed access to it on certain terms. A temporary licence could be granted for example to a private company providing security services. Suomen Erillisverkot Oy, who is in charge of the licences, scrutinise each case separately before granting the right to use VIRVE. Using the network does not necessarily mean access to any of the talk groups ("channels") used by authorities (Suomen Erillisverkot Oy 2008).

In practice, the only way for private security providers to gain access to TETRA is to borrow handsets from public authorities. Even then there are not always enough handsets available for the biggest events. Without equipment there is no uniform and unhampered communication across organisations. The terminals are too expensive to purchase for one single event. Even renting them is costly because of their high rent rates which exceed the purchase price in a couple of

days. Thus, handset terminal rentals are not financially feasible if no there is no incentive to do so (Orakoski 2008).

Even though it is possible to receive simultaneously several talk groups with a TETRA handset, in practice it is not always possible in a management situation. Monitoring even as many as two talk groups proves too challenging with regard to the enormous amount of messages, especially during a crisis. In the rescue organisation plan it was mentioned that a manager operating at the Stadium needs two handsets in order to handle the defined talk groups. Technical communication between groups had thus, in a way, been noticed - at least in one instance.

Communication Planned For Authorities

Among the authorities the communication instructions and the use of VIRVE is routine. Since the private sector only rarely use VIRVE, communication planning, which includes private security providers, has been neglected. Only on a few occasions have there been scenarios in which the use of VIRVE by the private security sector has been noted.

Our interview study indicated that some public officials have difficulties in accepting that the authority network can be used by other organisations as well. They do not seem to appreciate all the benefits of the use of TETRA network. Some even seemed to suspect that VIRVE talk groups can be eavesdropped so that confidential information is in danger “insider risk” (Pursiainen etc. 2007, 95)). This is not at all likely technology-wise but weighing the legal ramifications of “overhearing” against the effective distribution of information may be something to consider in a joint command centre environment.

Laws, Degrees and Acts

For this study case we focused research on some of the laws fundamental to the cooperation between various authorities in Finland. The duty of each authority to provide executive assistance is decreed separately by law. Each authority has a duty to provide and a right to receive executive assistance. In addition, each authority has the right to engage persons to assist, if the situation so warrants.

There is no uniform legislation concerning the relations between authorities and private security services. This expert opinion was confirmed by the Research Service of Parliament. Only in a section of the Constitution of Finland are these relations mentioned. However, even this section, of course, does not apply to event security as such. A private security provider is not defined in any legislation as a provider or receiver of executive assistance.

There is however the relationship between public and private that stems from the legislation – the supervisory role that authorities have. In events it is also a dual role as they are at the same time both the actor whom should be working shoulder to shoulder with the private colleagues but while also overseeing simultaneously that the stipulations of permits and regulations are met. So, according to the law, private security actors are considered separate and having no interface with public authorities other than in regulatory settings. This mostly works fine with smaller events but disregards the needs of the likes of our case study.

As declared, the aforementioned legislative situation is based on the situation in Finland. Since the initial research, a ministry workgroup to develop legislation in this field in Finland was initiated. There is reason to believe that similar situation regarding private security exists in most countries (Button 2008). Co-operation has been deemed one sided or perhaps even been left undefined.

The "Bigger Picture" of Interaction, Co-Operation and Social

The big picture in all this is how should the parties involved interact, co-operate and, in some ways, integrate. The grander picture is where we have to contemplate what societal and human needs, wants, requirements and risks and opportunities are at stake.

The Economics of Resources

There is a logic that supports integration and co-operation; the logic of economics and scarcity of resources. It is precisely in large events that the need to co-operate is underlined to use the human and other resources available in the most feasible manner possible. In shared and co-operative management human resources are the unit of interest and communication in interaction between humans. The Helsinki games could not have been made without participation across organisational limits.

The smart deployment and effective use of scarce resources is only half of the story. The other is to understand the somewhat mechanical thought sensory activity that all security and safety personnel are engaged in. They all act as sensors to feed information to a command and communication nexus: normal activities, abnormalities and more serious security concerns. They not only serve as first responders but also create a larger distributed network than that any single organisation could. The different groups involved feed information into the system, dissect it, add their own expertise to others and accumulate tacit knowledge about the event. Shared knowledge then supports satisfactory results through the enhanced speed and quality of work (Probst, Raub & Romhardt 2000, 170). Such synergy benefits are critical for preventative measures as well as after the fact efforts.

As important as security and safety are, they are still support activities and structures for society, economy and events. Economically, as well as per individual events, joint operations create efficiency and thus safety and security (or at least the image of). This is a real advantage that international events look for in a venue. This point can be noted from the reports about the Helsinki games application process (MTV3 2002) as well as from the report from Ministry of Education about the national strategy for major international events (Linna, Hakala-Zilliacus & Tolonen 2006, 34-36)

The Trust Issue

Trust is the base that every joint- and co-operative action is built on. A simplistic way to estimate trust is "either-or" or "trust/distrust", the black-or-white binary pair, which rarely describes the actual situation accurately. For security and safety to actualise and function, there has to be some level of trust towards the general public, audience, the (paying) customer as well as performers and other staff.

For any kind of meaningful interaction to exist, there has to be some ba-sic level trust towards the other. The security guard expects to be taken seriously by the authorities as well as the other way around. The basic level of trust is interwoven in the roles we have and take while interacting. Mostly these are social norms but in some cases these expectations may be written down as guidelines or law - contracts of sort. Whether written down or not, these are the generally excepted norms by which we set our trust (Tourish & Hargie 2004, 12-13).

The general acceptance of these social contracts makes them formal and thus they can be called formalised trust. This is the level of trust we usually operate between people and organisations we do not really know. Sometimes a situation is even hindered by the fact that we do not fully understand the extent, specifics and dynamics of an applicable contract. Thus we keep to the parts that are simple, clear and understood - while at the same time enforcing the idea of them to be the most central parts of a vague contract, pushing it inadvertently askew from its originally intended form. In communication theory this is termed “uncertainty avoidance” (which is not the same as risk avoidance). Uncertainty avoidance means unspecified, unclear and unpredictable are avoided and strict codes of behaviour and absolute truths are used or at least preferred (Turner 1999, 490; Hofstede 1994, 163-172, 260, 263).

The basic interaction is based - and limited - on the trust framed by the contract between organisations. If the individual has some experiences with the other organisation or individuals, that will come in to play either as a positive or negative. Personal experience based trust is the most common informal form of trust. Informal trust is often gained by doing things together, creating an understanding

of a common language (jargon) and the working methods of all involved (Probst etc. 2000, 192-194, 276-277).

Formal trust is often forced and rarely flexible. Trust between organisations is mostly formalised and the formal level is easily seen as the maximum. An example of this is to limit the access and communication to formal channels and methods (although sometimes organisational and technical systems set similar requirements but that should not be mistaken here). Informal trust stems from actually knowing the other and is usually stronger but more prone to fluctuation. The gap between the required level of trust, for example, on the cooperative use of resources, and the level found can be overcome (at least locally) by personal informal trust. Both of the aforementioned examples and their reasons were present in our examined case. Informal trust was accepted as a sufficient level to form joint security management in the areas that were seemingly most efficiently and smoothly run. Similar findings on informal knowledge sharing were reported in (Jarvenpaa, Majchrzak 2008, 260-276).

The Experience Issue

Legislation does not define the security providers in the private sector as an official operational partner. The public authorities are not always aware of the capacities and knowhow of the private security sector. Most of them lack personal contact with private security management and planning professionals. Instead, many of them perceive the private security branch only as security guarding and have little experience of working with security guards.

The public authorities, especially police and fire rescue, are highly trained and their expertise is revered almost without question. However, this may have developed blindness on an individual level to the fact that the public authorities lack special expertise and experience with regard to event security, which differs from their daily functions. Hard security approach goals cannot be accomplished without also taking care of soft security needs. Vice versa, soft security must also prepare for risks that can only be tackled by the hard security approach. Incidents themselves within events are basically similar regardless of the setting but the event setting does generate new challenges that affect how these incidents can and should be approached. One could even speak of “project security”.

There are individual public authority members that are especially knowledgeable and experienced from having worked with events but even then that knowledge does not spread effectively. Some localities also benefit by having a yearly large event but a few large events a year do not ensure expertise. Even within private security there is similar division as one should not expect a doorman or a shopping centre guard to be keenly aware of the intricacies involved in working at a large event. Private security in general has the advantage in learning by doing

more, especially with reference to events. This is in contrast to authorities taking part in event security operations (besides the permit process). In fact, the authorities become involved after some incident has occurred, which results from working separately in the first place.

All security actors should acknowledge each other's proficiency and capabilities. Furthermore, to be able to effectively work together this needs to be rehearsed (Zarraga & Bonache 2003, 1238-1240; Das & Teng 1998, 504-509).

Suggestions and Conclusions

Seamless communication is the key when providing security at public events. Our case study suggests possibilities for improvement and acts as a reminder to all who are planning a large event.

A good Structure for an Organisation's Activities

Different agencies - including those in the private security sector - should have predefined operations models and compatible equipment in order to fulfil effective communication. A carefully prepared communication plan involving all the security providers, private as well as public, should have special emphasis on communicating across organisational boundaries. Even more so if the organisations and their members are rarely in contact with each other.

A great part of the activities requiring communication takes place in the actual event area between actors on the same level. However, an emergency or a threatening situation requires centralised management and proper support for it and a common command and communications centre for all the security providers, similar to that in the studied case.

Regulatory and Legislative Enhancements

All security actors are currently seen still as somewhat separate in the field of total security - despite political level integration efforts everywhere. Even in Finland, which has been considered as a prime example of different agencies working together, there is still a clear "segregation of roles". A holistic framework for total security is missing that would better define different organisational interaction, especially in a joint operation at a large event such as Helsinki 2005 was.

At some level interaction and co-operation may be an "extra legal" non issue, but by updating the legislation, a homogeneous operations model could be created. In particular, the role of the private security provider should not have to be dependent upon the diverse methods and routines of different organisations as it is

under the current system in Finland and many other countries. Thus, for example communicating in the same authority network and the presence of the management of the private security companies in the operational command centres should be based on law and not on the unofficial practices of different authorities. This would guarantee a continuous and swift flow of information in the emergency situations in a way it has been customary between authorities in providing and requesting executive assistance at large-scale incidents. Such regulatory support for the integration of intentions could boost longer term co-operation planning.

Attitude Adjustment and Training

Genuine trust that also tolerates minor faults is something far deeper than trust based on law, and usually requires a personal level of familiarity. This manner may not be easily changed but the level of current trust and familiarity with each security actor's competence can be raised. Ways to tackle this are large joint exercises; specific courses on the subject together with other security actors; an exam/audit system for private security individuals operating at management level; and new guidelines and/or legislation to support joint activities better. Some combination is most likely needed.

Should formal mechanisms not be possible or, as bureaucracy is slow, new legislation and systems take time, informal levels of trust can be enhanced as well. Seminars, recurring meetings; local or event related drills; and generally working together in genuine cooperation – not just side by side – in a manner where all learn from previous experience and share their knowledge with their respective organisations will help address the issues raised. With these actions underlying attitudes can be changed, if they are promoted decisively, and especially if they are carried out prior to a common task – the next large event to be handled jointly.

Conclusion

In this research we touched only on some themes that emerged as points to consider and develop. The issue mainly concerned the effectiveness of command and control room operational management and its communication. The best technologies are seen to be useless if they are not used right and they will not be effective if co-operation is not trained for planned and agreed upon beforehand. Laws and regulations can be used to give a homogenous form to the methods and interaction used, a readymade basis that can be built depending on what kind of event is in question and what kind of security organisation it needs.

To take this research further, it is proposed that a similar review could be made regarding situations in other countries about 1) current methods of handling ex-

ceptionally large events and the use of communication technology to support them; 2) laws and regulations governing this topic and whether meaningful co-operation in this context is supported; and 3) the level and type of interaction and co-operation between all the security actors. The size of an event may be relative but the type could be any event not just one held yearly in the same location.

References

M. Button, Institute of Criminal Justice Studies, University of Portsmouth, presentation and discussion at Laurea 2nd International Security Management Seminar, Laurea University of Applied Sciences, Espoo, Finland, April 17th 2008.

T. K. Das, B.-S. Teng, “Between trust and control: Developing confidence in partner Cooperation in alliances” Academy of Management Review Vol. 23, pp. 504-509, No. 3, 1998.

K. Heikkonen, T. Pesonen, T. Saaristo, You and Your Tetra Radio. Helsinki, Finland: IT Press, 2004.

G. Hofstede, Cultures and Organizations - Intercultural Cooperation and its importance for survival. London, England: HarperCollins, 1994.

J. Hänninen, “Poliisi valmistautuu MM-kisoihin” in Poliisilehti, vol.3, 2005 [Online]. Available: http://www.poliisi.fi/poliisi/poliisilehti/periodic.nsf/vwarchivedlist/106B5DBB004FC9EDC22570130033BB2E

E. Juholin, Communicare! (4th ed). Porvoo, Finland: Inforviestintä Oy, 2006.

S. L. Jarvenpaa, A. Majchrzak, “Knowledge Collaboration Among Professionals Protecting National Security: Role of Transactive Memories in Ego-Centered Knowledge Networks”, Organization Science, Vol. 19, pp. 260-276, March 2008.

E. Kaukonen (2005, May 25). Pelastustoiminnan johtaminen. Kuopio, Finland: Pelastusopisto 2005 [Online]. Available: http://www.pelastusopisto.fi/pelastus/images.nsf/files/E930C15689A09493C22571E3003AD816/$file/Johtamisopas.pdf

M. Linna, L.-M. Hakala-Zilliacus, H. Tolonen, Report of the Committee on a national strategy for major international events in Finland. Ministry of Education, Finland, 2006, pp. 34-36 [Online]. Available: http://www.minedu.fi/export/sites/default/OPM/Julkaisut/2006/liitteet/tr27.pdf

S. Orakoski, VIRVE Tuotteet ja Palvelut Oy, Espoo, Finland. Private communication, March 18th 2008.

A. Pinnington, “Organizational culture: Liberation or entrapment” in Key Issues in Organizational Communication, D. Tourish and O. Hargie, Ed. New York, USA: Routledge, 2004.

G. Probst, S. Raub, K. Romhardt, Managing Knowledge: Building Blocks for Success. Chichester, England: Wiley, 2000.

C. Pursiainen, P. Lindblom, P. Francke, “Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection” Nordregio, Stockholm, Sweden, report 5, 2007.

P. S. Shockley-Zalabak, Fundamentals of Organizational Communication: knowledge, sensitivity, skills, values (7th ed). Boston, USA: Pearson/Allyn&Bacon, 2006.

D. Tourish, O. Hargie, “The Crisis of Management” in Key Issues in Organizational Communication, D. Tourish and O. Hargie, Ed. New York, USA: Routledge, 2004.

R. J. Turner, The Handbook of project-based management: improving the processes for achieving strategic objectives (2nd ed). London, England: McGraw-Hill, 1999.

Virve – turvattu yhteys, Suomen Erillisverkot Oy. (2008, December 11) [Online]. Available: http://www.erillisverkot.fi/index.php?id=20

Yleisurheilun MM-kisat Suomeen, MTV3 (2002, April 15) [Online]. Available: http://www.mtv3.fi/uutiset/arkisto.shtml/arkistot/kotimaa/2002/04/108668

C. Zarraga, J. Bonache, “Assessing the team environment for knowledge sharing: an empirical analysis” International Journal of Human Resource Management, vol. 14, pp. 1238-1240, Nov. 2003.

Chapter 13
Nuclear Security at Public Events and Political Meetings

The Use of Indoor Positioning System for the Security Arrangement of Radiation Sources

Jari Syrjälä

Master's Thesis, Laurea University of Applied Sciences, 2009.

The Radiation and Nuclear Safety Authority of Finland (STUK) has taken advantage of Global Positioning System technology with respect to radiation level measurements. For the indoor positioning of radiation sources, however, the GPS technology is not applicable due to the lost of direct line of sight to satellites.

Indoor positioning is mainly used in industry and healthcare. Within industry it is mostly used for tracking goods and within healthcare for locating equipment and people. The indoor positioning systems on the market today are based on the fingerprinting method which utilises existing wireless LANs. When applying the fingerprinting method, the calculation of the location of an item is based on the measurement of the received signal strengths of the wireless LAN's action points.

The goal of this master's thesis was to study the positioning systems which are based on the fingerprinting method in general and their suitability for locating radiation sources. The applicability of the fingerprinting method was evaluated by using the equipment and software provided by Cisco Systems and Ekahau Inc. The objective of this thesis was to evaluate how the fingerprinting method could be applied to locate radioactive sources.

The methodology followed in this thesis is the one typical to the applied sciences. The starting point for the study was to setup a well known construction within the STUK premises, since the contribution of this study was not to prepare any new indoor positioning systems but, to study its applicability for locating radioactive sources. In this M.A. thesis, the scientific literature and technical articles dealing with the indoor positioning technology were studied and form the theoretical basis of the study.

In this work the required measuring environment was established for locating radioactive sources. The applied part of the thesis set up an application for binding together the radiation measurement data and location data in the database and, for representing the results on building layout plan.

This study was able to demonstrate that it is possible to track radioactive sources by utilizing indoor positioning systems based on a wireless local area network. However, due to the very laborious and time consuming implementation of the indoor positioning systems using the fingerprinting method, the conclusion is that they are not well applicable for tracking on an ad-hoc basis, in which the fast set up of a system in an unfamiliar environment is a very basic requirement.

Indoor Positioning for Nuclear Security

Jolanta Garlacz

Master's Thesis, University of the West of Scotland, 2009.

Abstract: In this research project, an existing real-time location system based on multiple Wi-Fi signals was developed for use as an Indoor Positioning System. A Java application, IPARM, was created in cooperation with the Finnish Radiation and Nuclear Safety Authority, with the aim of reducing or removing human error from the accurate positioning of measurement equipment within buildings. The effectiveness and accuracy of the system was estimated and found to be beneficial for use in equipment monitoring during radiological emergencies.

Introduction: The undertaken project will evaluate the benefits of using an indoor positioning system to support nuclear security in indoor environments. To investigate available indoor systems, carefully study on existing solutions has been done. The next chapter presents a critical review of the current state of publications regarding indoor positioning systems and possibilities of their application. After analysis, the Ekahau Real-Time Location System (RTLS) has been chosen as an indoor positioning system. Ekahau is a Finnish company specialising in indoor positioning systems.

While searching for new possibilities for applying the Ekahau RTLS, radiation measurement has been taken into account. Nowadays, radiation levels are monitored all over the world. The Finnish Radiation and Nuclear Safety Authority (abbr. STUK) monitors radiation levels in Finland. They possess specialist equipment for measuring radiation levels. They agreed to provide a portable radiation-measuring unit for the purpose of testing. The project intends to implement the indoor positioning system to the portable radiation-measuring unit. For that reason, a java application - IPARM – has been created.

The research is a ‘technology demonstration’ that will be tested in an indoor environment. The main aim of the thesis is to find the benefits of applying a WLAN based indoor positioning system to a portable radiation measuring unit. The research is based on an internship at the Laurea University of Applied Sciences, Leppävaara, Espoo, Finland.

Indoor Positioning for Nuclear Security

Tarja Ilander, Harri Toivonen, Ulf Meriheinä, Jolanta Garlacz

In the Proceedings of Third European IRPA Congress 2010 June 14−16, Helsinki, Finland.

Abstract: Mobile measurements are needed to search for nuclear material not under regulatory control at major public events and political meetings. The mobile measurement teams may have to screen hotels, living quarters and other venues before an event and during the event. Measurement and positioning information are crucial for planning such missions and for reporting findings.

Traditionally the global satellite navigation system is used for positioning outdoors. Positioning indoors is difficult. Various indoor positioning technologies are available on the market. However, they often need a specific infrastructure installed in a building which limits their use.

The Radiation and Nuclear Safety Authority (STUK) has performed indoor positioning tests with Ekahau’s wireless network based system. The experiences with the field tests were encouraging. Also a novel indoor positioning system has been developed by VTI Technologies. In this system navigation is based on the measurement of the length and direction of every step of a person. It uses a chest-worn speed and distance measurement module, originally developed for the sports market, together with an instrument-grade gyroscope and a magnetometer.

Chapter 14
School Shootings and other Crisis Situations

Behavioural Threat Management: The Prevention of Severe Targeted Violence at Educational Institutions

Peter Sund

Master's Thesis, Laurea University of Applied Sciences, 2009.

Severe violence in schools and other educational institutions has become a rising concern in many developed countries in recent years, especially in the U.S. and Europe. This is due to the devastating violent attacks that have occurred across a wide range of western educational institutions. There has been much discussion about how to deal with this issue. However, a large part of the discussion has been directed towards general problems in society, cultural changes and of course how to react to the attacks when they occur and what to do afterwards. These questions have initiated a notable amount of different development projects. Consequently, not many of these projects have been concentrated on the tactical and operational level of prevention, specifically on precise and timely prevention of severe targeted school violence.

This thesis is a report of constructive research on the behavioural threat management process of educational institutions. It is tied to the larger aim of an action research project within the Finnish educational system to learn more about the implications of the process. The goal of this thesis was to develop a model of the behavioural threat assessment and management process for educational institutions in the Finnish educational system; In other words to recognise, access and manage risks concerning the occurrence of severe violent behaviour in school like environments. The model was constructed through the utilisation of a comprehensive literature analysis and thematic expert interviews.

This paper is meant to fill the gap — the relatively short timeframe — be reactive security measures implemented during and after an attack and the early intervention measures tackling the origins of risk related to school attacks. The preceding argumentation documents that there is an effective way to fill this gap; it's called behavioural threat management. This proactive approach seeks to identify and manage students threatening severe targeted violence.

Furthermore, within the developed contemporary threat management model, the pathway to violence is incorporated for the first time to consider risk mitigation strategies in the context of targeted school violence. The strategy encompasses

both multi-professional and cross-organisational cooperation in the assessment and management processes. Additionally, the whole process is embedded into the standard operating procedures of a school.

Responsibility and Decision Making Transfer for Public Safety and Security Emergencies - A Case Study of a School Shooting

Jukka Ojasalo, Tuomas Turunen, Hanna-Miina Sihvonen

In the Proceedings of the IEEE International Conference on Technologies for Homeland Security (HST 2009), May 11-12, 2009, Boston.

Abstract: The purpose of this study is to increase the knowledge of responsibility and decision making transfer in public safety and security emergencies. The vast amount of literature dealing with emergencies includes surprisingly little empirically grounded knowledge of responsibility and decision making transfer in emergency management. The article is based on the case study method in the context of school shootings. The contribution of this article relates to the following findings. Firstly, most of the decision making in the emergency examined is ad hoc and situation driven. Secondly, effective operation requires that the on-scene-commanders of different authorities and organisations share the same on-scene-command post or the same situational awareness - preferably in real time. Thirdly, the first authority, or the first law enforcement patrol, etc., reaching the scene in a time critical emergency, usually has a paramount role in developing and implementing a solution to the situation. Several management approaches are suggested related to these three findings in order to make responsibility and decision making transfer more efficient and effective in emergency management.

Communication, Information -Transfer and Role -Shifts in a Challenging Public Safety and Security Field Operation

Tuomas Turunen

Master's Thesis, Laurea University of Applied Sciences, 2010.

Criminal incidents, such as the high jacking of a ship in international waters or a multiple homicide in a school, require effective action from all safety and security organisations involved. Many rescue and law enforcement operations require a transfer of information during a change of personnel from morning shift staff to evening shift staff, for example. This exchange is referred to as role shifting. In the case of a high-jacked ship, role shifting may become complicated as the op-

erational area and context may change from one country to another or to international waters as the ship continues its journey. The issues of transferring information and role shifting during a multi-actor operation are the focus of attention in this study. In this thesis a model for managing a complicated operational entity is constructed that addresses the issues of acquiring and disseminating facts, role-shifting, effective decision-making, and managing related risks.

In this thesis the acquisition and dissemination of facts, role shifting and managing related risks are studied from the perspective of different operations in the public safety field as well as from the perspective of actors with personal experience and professionals in the field. The context of all the above mentioned is an operational entity, which in the best cases consists of planning, action and the post-action phases. The operations may be in response to natural or manmade disasters that may be long-term or short term and require decision making delegations and role shifts due to their dynamic nature and rapidly changing conditions and environment.

The government officials working in such operations usually follow a predefined command and control model in which the decision making is the duty of high-ranking officials. One needs information to effectively make a decision. Even in modern society an inability sometimes exists, due to either technical or human reason, which prevents the expeditious transfer of necessary information. In many time-critical, life-threatening and rapidly changing situations (an operational entity) decisions must be made in a split-second and often on the frontline. Therefore, time constraints do not allow for decision making to follow the chain of command; decisions must be made in an ad hoc way depending on the situation.

Towards the Transparent Authority of Power in Law Enforcement

Jouni Viitanen, Pasi Patama, Juha Knuuttila, Jyri Rajamäki, Harri Ruoslahti

Security in Futures – Security in Change, The 12th Annual Conference of the Finland Futures Research Centre and the Finland Futures Academy, 3–4 June, 2010, Turku, Finland.

Abstract – To prevent and investigate crimes, Law Enforcement Agencies (LEA) conduct various operations which affects the privacy of citizens. These activities include such controversial areas as video surveillance, audio surveillance and technical tracking. Currently, the LEA has the power to conduct these operations based on legislation. Furthermore, law enforcement is applying more jurisdiction based rights in order to open up new frontiers, which could intrude even further into ordinary citizen's privacy. Consequently, public concern is rising and openly

discussing: Do LEAs really need more powers of surveillance? Are they exercising given powers according to legislation? Is there a balance to be found between LEA's operational security needs and individual freedoms? These questions have been raised by civil rights activists opposed to the increasing surveillance conducted by the state. This paper outlines a scenario how of common ground can be found with a constructive approach that can be facilitated by advanced technology.

List of Publications

Journals

Rauno Pirinen, Jyri Rajamäki, Lili Aunimo, Rescuing of Intelligence and Electronic Security Core Applications (RIESCA), In WSEAS TRANSACTIONS on SYSTEMS. Volume 7, 2008 ISSN: 1109-2777.

Jyri Rajamäki, Tuomas Turunen, Aki Harju, Miia Heikkilä, Maarit Hilakivi, Sami Rusanen, Face Recognition as an Airport and Seaport Security Tool, In WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, Issue 7, Volume 6, July 2009.

Jyri Rajamäki and Timo Villemson, Creating a Service Oriented Architectural Model for Emergency Vehicles, In INTERNATIONAL JOURNAL OF COMMUNICATIONS Issue 2, Volume 3, 2009.

Conference Papers

Rauno Pirinen and Jyri Rajamäki, Modeling and Simulation of Critical Infrastructures Case: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA), In the Proceedings of The 2nd EUROPEAN COMPUTING CONFERENCE (ECC'08) Malta, September 11-13, 2008, ISSN:1790-5109, ISBN: 978-960-474-002-4.

Jouni Viitanen, Pasi Patama, Juha Knuuttila, Jyri Rajamäki, Harri Ruoslahti, Towards Transparent Authority of Power in Law Enforcement, Security in Futures – Security in Change, The 12th Annual Conference of the Finland Futures Research Centre and the Finland Futures Academy, 3–4 June, 2010, Turku, Finland.

Jyri Rajamäki, Tuomas Turunen, Aki Harju, Miia Heikkilä, Maarit Hilakivi & Sami Rusanen, Facial Recognition System as a Maritime Security Tool, In Proceedings of the 8th WSEAS International Conference on Signal Processing Istanbul, Turkey, May 30 - June 1, 2009, ISSN: 1790-5117, ISBN: 978-960-474-086-4.

Jouni Viitanen, Markus Happonen, Pasi Patama, Jyri Rajamäki, International and Transorganisational Information Flow of Tracking Data, In Proceedings of the 8th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP '09) Puerto De La Cruz, Tenerife, Canary Islands, Spain December 14-16, 2009 ISSN: 1790-5117, ISBN: 978-960-474-143-4.

Pasi Kamppi, Jyri Rajamäki, Robert Guinness, Information Security in Satellite Tracking Systems, In Proceedings of the 3rd International Conference on Communications and Information Technology (CIT'09) Vouliagmeni, Athens, Greece December 29-31, 2009, ISSN: 1790-5109, ISBN: 978-960-474-146-5.

Jyri Rajamäki, Timo Villemson, Designing Emergency Vehicle ICT Integration Solution, In Proceedings of the 3rd International Conference on Communications and Information Technology (CIT'09) Vouliagmeni, Athens, Greece December 29-31, 2009, ISSN: 1790-5109, ISBN: 978-960-474-146-5.

Tarja Ilander, Harri Toivonen, Ulf Meriheinä, Jolanta Garlacz, Indoor Positioning for Nuclear Security, In the Proceedings of Third European IRPA Congress 2010 June 14−16, Helsinki, Finland.

Jukka Ojasalo, Tuomas Turunen, Hanna-Miina Sihvonen, Responsibility and Decision Making Transfer in Public Safety and Security Emergencies -A Case Study of School Shooting, In the Proceedings of the IEEE International Conference on Technologies for Homeland Security (HST 2009), May 11-12, 2009, Boston.

Master's Thesis

Marjo Nissilä, New ICT Supply Process, Interfaces between Supply Process and Project Management Process in ITIL Service Design Framework, Master's Thesis, Laurea University of Applied Sciences, 2009.

Teija Mikkola, Person's strong electronic identification, Master's Thesis, Laurea University of Applied Sciences, 2009.

Jani Arnell, Development of the Finnish Communications Regulatory Authority's Enterprise Risk Management, Master's Thesis, Laurea University of Applied Sciences, 2010.

Kimmo Syrjänen, Maturity modelling as a catalyst for IT continuity management implementation in a large company, Master's Thesis, Laurea University of Applied Sciences, 2009.

Markus Lalla, Building the foundations for information and communications technology continuity management in a merger based company, Master's Thesis, Laurea University of Applied Sciences, 2009.

Sami Rusanen, Management of common security, Master's Thesis, Laurea University of Applied Sciences, 2009.

Jolanta Garlacz, Indoor Positioning for Nuclear Security, Master's Thesis, University of the West of Scotland, 2009.

Jari Syrjälä, The Use of Indoor Positioning System for the Security Arrangement of Radiation Sources, Master's Thesis, Laurea University of Applied Sciences, 2009.

Peter Sund, Behavioral Threat Management: Prevention of Severe Targeted Violence in Educational Institutions, Master's Thesis, Laurea University of Applied Sciences, 2009.

Tuomas Turunen, Communication, Information Transfer and Role-Shift in a Challenging Public Safety & Security Field Operation, Master's Thesis, Laurea University of Applied Sciences, 2010.

RIESCA

In the RIESCA project (The Rescuing of Intelligence and Electronic Security Core Applications) Laurea aimed at developing further evaluation methods for systems that are critical to the functioning of the society. The aim of the RIESCA project is addressed to analyse of methods, which could contribute processes of evaluation and the continuous system's development. Special attention was given to the analysis of moving from situations of normal activity to critical situations, and studying how such systems could be recovered from their crisis state and returned to their normal state. A further aim was to develop different scenarios related to critical events (mass events, high level political meetings, crisis situations), security management and communication systems and assesses various methods for evaluating their functionality.

During the project Laurea's researchers and students, as research colleagues in co-operation with other RIESCA project researchers, analysed existing standards and methods, and evaluated their applicability for the evaluation and development of critical systems and event security management. The target of the project was to create a process that could evaluate and develop security management for critical systems and events. This was done by making as much use of existing methods and standards as possible. The pilot projects concerning these methods were mostly carried out with organisations that took part in the project. The whole process (operations model) was supplemented by solutions that were developed during the project.

This report is a record of the output of the RIESCA project and serves as a 'toolbox'; a series of procedures for the evaluation and development of critical systems and event security management.

ISSN 1458-7238
ISBN 978-951-799-206-0

LAUREA

www.laurea.fi